CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 118 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 2 octobre 2018

Président

M. Bob Zimmer

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le mardi 2 octobre 2018

● (1105)

[Traduction]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bienvenue à la 118e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément au sous-alinéa 108(3)h)(vii) du Règlement, nous poursuivons notre étude sur l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook.

Aujourd'hui, nous entendrons les témoins Elizabeth Dubois, Michael Pal et Samantha Bradshaw.

Nous donnons d'abord la parole à Mme Dubois, pour 10 minutes.

Mme Elizabeth Dubois (professeure adjointe, Département de communication, Université d'Ottawa, à titre personnel): Bonjour. Je vous remercie de m'avoir invitée à témoigner devant vous aujourd'hui.

Je suis professeure adjointe à l'Université d'Ottawa. J'ai obtenu mon doctorat à l'Université d'Oxford. Mes recherches portent sur la communication politique dans l'environnement des médias numériques. J'ai examiné des enjeux comme l'utilisation de l'intelligence artificielle et des robots en politique, les chambres d'écho et la perception qu'ont les citoyens de l'utilisation des données des médias sociaux par des tiers comme des gouvernements, des journalistes et des partis politiques.

J'ai fait de la recherche au Canada et à l'étranger, mais aujourd'hui, je vais me pencher sur quatre facteurs. Premièrement, je vais comparer les stratégies analogique et numérique du ciblage des électeurs. Deuxièmement, je vais décrire la modification des définitions des publicités politiques. Troisièmement, je vous parlerai de l'autoréglementation des plateformes et quatrièmement, je traiterai de l'intelligence artificielle.

Tout d'abord, je tiens à souligner qu'en mentionnant le terme « plateforme » tout au long de mon témoignage, je désignerai les entreprises de plateformes technologiques comme les médias sociaux, les moteurs de recherche et autres.

Commençons par le ciblage des électeurs. Ce phénomène n'a rien de nouveau. Toutefois, il évolue à un rythme spectaculaire. En général, les partis politiques trouvent très utile de recueillir de l'information en faisant du porte-à-porte pour demander aux gens s'ils ont l'intention de voter et pour qui. Certains demandent aussi aux citoyens quels enjeux les préoccupent. Les partis peuvent ainsi mieux orienter leurs ressources, qui sont limitées. Cette stratégie rapproche aussi les citoyens du système politique.

La stratégie analogique risque cependant de désengager certains électeurs et de les écarter du processus. Par exemple, si certains groupes semblent peu disposés à voter, ils risquent d'être ignorés pendant tout le reste de la campagne.

La collecte de données numériques peut amplifier ces problèmes et présenter de nouveaux défis. Je vois quatre grandes différences entre la stratégie numérique, qui ne cesse de se développer, et l'approche analogique que je viens de décrire.

Premièrement, les données numériques et analogiques sont très différentes. On recueille maintenant les données avec une rapidité et une portée incroyables. Même si la collecte de données nécessitait autrefois beaucoup de ressources humaines, elle se fait maintenant automatiquement au moyen d'outils extrêmement complexes. Je crois que la semaine dernière, vous avez entendu plusieurs témoins décrire ceux que les partis politiques utilisent à l'heure actuelle.

De même, il est maintenant plus facile de joindre ces données à d'autres ensembles de données, comme les antécédents de crédit et d'autres renseignements personnels. Les citoyens ne permettraient peut-être pas à des partis ou à des entités politiques d'utiliser ces renseignements. En outre, il est plus facile d'échanger, de transmettre et d'analyser ces données. On peut effectuer des analyses prédictives grâce à l'énorme volume des données recueillies. On dispose de beaucoup plus de types de données que l'on peut réunir et analyser très rapidement.

Deuxièmement, il est très possible que les citoyens ne sachent plus que l'on recueille leurs données pour les utiliser. Contrairement à l'époque où ils devaient répondre à la porte pour donner des renseignements personnels, on peut maintenant le faire à leur insu. Ils ne savent peut-être même pas ce que la technologie nous permet de faire. Les résultats d'une étude sur les internautes canadiens que mes collègues de l'Université Ryerson et moi-même avons menée indiquent que la plupart des Canadiens n'aiment pas que des partis politiques se servent des données que tout le monde trouve aisément dans les médias sociaux. Pour moi, cela indique qu'il serait crucial de déterminer le genre de données que les citoyens voudraient que leurs représentants politiques aient et utilisent.

Troisièmement, l'utilisation des données évolue. Comme les publicités en ligne, par exemple, peuvent maintenant cibler des auditoires très particuliers, les données personnelles sont devenues plus utiles aux entités politiques. Cette utilisation est cependant moins transparente pour les organismes de réglementation et moins claire pour les citoyens. Les approches émergentes risquent donc d'enfreindre les lois en vigueur, mais elles sont tellement difficiles à retracer que personne ne s'en aperçoit. Pour intervenir efficacement, il sera crucial d'accroître la transparence et la reddition de comptes.

Quatrièmement, les entités politiques sont poussées à recueillir des données continuellement et non uniquement pendant les campagnes électorales. Les lois électorales en vigueur risquent donc de ne pas suffire. Soulignons en outre que les partis politiques ne sont pas seuls à recueillir ce genre de données. Les organismes sans but lucratif, les syndicats et d'autres tierces parties le font aussi, de sorte que nous ne pouvons pas limiter l'examen de la collecte et de l'utilisation des données aux partis politiques en général.

Ces changements sont particulièrement préoccupants, car bon nombre de ces utilisations ne sont pas prévues dans les lois actuelles sur la protection de la vie privée. De plus, le Commissariat à la protection de la vie privée n'a pas les outils nécessaires pour veiller à ce que ces lois soient appliquées comme elles le devraient.

Toutefois, cette utilisation des données n'est pas toujours néfaste. Elle contribue à accroître le taux de participation des électeurs en les éveillant de leur apathie. Cela dit, pour équilibrer le pour et le contre, il sera crucial de viser aussi les partis politiques dans les lois sur l'utilisation des données personnelles en vigueur, surtout dans la Loi sur la protection des renseignements personnels et les documents électroniques. Il faudra y ajouter des dispositions sur la transparence et sur la reddition de comptes de l'utilisation politique des données. Il faudra également éduquer les citoyens en créant par exemple des déclarations de consentement mieux éclairées et en lançant des initiatives de littératie sur les médias et sur la culture numérique.

Je vais consacrer les minutes qu'il me reste à quelques problèmes que suscite cette approche de ciblage des électeurs. Citons d'abord la publicité politique. Elle n'est plus aussi évidente qu'auparavant. Outre le coût du placement de ce que les plateformes considèrent souvent comme de la publicité, les entités politiques ont toutes sortes d'autres moyens d'afficher leur contenu payant dans le fil de nouvelles d'une personne ou dans une vidéo recommandée. Elles peuvent aussi manipuler les algorithmes pour faire apparaître certains éléments de contenu à l'écran des gens.

Elles peuvent y lancer des histoires commanditées, engager des ambassadeurs de marque, louer des comptes déjà très populaires dans les médias sociaux ou utiliser des bots politiques pour diffuser l'information à plus grande échelle. Tout cela se fait soit gratuitement, soit sur une base payante, et dans ce dernier cas, cela ressemble beaucoup à de la publicité selon l'esprit de la loi.

Pour contrer cela, il faut redéfinir ce qui constitue une publicité politique afin que les lois en vigueur continuent à s'appliquer et à produire les résultats escomptés. Il sera particulièrement important d'en tenir compte en examinant l'augmentation fulgurante de l'utilisation des plateformes de messagerie instantanée partout dans le monde. Il est beaucoup plus difficile de suivre l'utilisation que font les partis politiques et d'autres entités politiques des plateformes de messagerie instantanée que des plateformes de médias sociaux, et ce problème ne pourra qu'empirer.

Deuxièmement, je veux parler de l'autoréglementation et du fait qu'elle est inefficace dans le cas des grandes plateformes. Elles ont réagi, mais de manière excessivement prudente. Elles n'ont pas réagi de façon proactive à la menace de la collecte et de la sauvegarde de données numériques et de renseignements personnels. Il faut tenir ces entreprises responsables du contenu qu'elles affichent sur leurs plateformes. Il faut également veiller à ce que leur manipulation de ces données soit transparente et responsable. À l'heure actuelle, on se heurte à une « boîte noire ». Nous ne savons pas comment les sociétés Facebook et Google décident de ce qu'elles permettent ou non que l'on affiche dans leurs plateformes. Cela ne peut pas durer alors que nous remettons en question les enjeux liés à la protection de la vie privée, à la propagande haineuse et à la liberté d'expression.

Enfin, l'utilisation de l'intelligence artificielle complique déjà beaucoup la situation. À l'heure actuelle, on nous fait croire que puisqu'on utilise des algorithmes d'apprentissage, il est impossible d'ouvrir cette « boîte noire » pour déballer et expliquer ce qui s'y passe. Cette affirmation ne s'applique qu'à une approche technologique très étroite, mais il est possible de prendre certaines mesures pour rendre l'utilisation de l'intelligence artificielle plus transparente et responsable.

Par exemple, on pourrait appliquer des processus d'essai plus clairs qui permettent aux gouvernements ou aux universitaires de vérifier les procédures. On pourrait vérifier régulièrement les algorithmes tout comme on audite des données financières. On pourrait exiger que l'équipe documente son élaboration des algorithmes, sa prise de décisions et qu'elle explique ces décisions. Il faut aussi étiqueter plus clairement les comptes automatisés dans les médias sociaux et dans les applications de messagerie instantanée et enregistrer les communications numériques automatisées avec les électeurs. On pourrait modifier le registre de communication avec les électeurs pour y inclure les contacts numériques automatisés. Il serait également crucial d'offrir des programmes de littératie numérique à grande échelle sur le fonctionnement de ces plateformes numériques afin que les citoyens soient en mesure d'exiger la protection que nous leur devons.

À mon avis, l'utilisation politique des données numériques a beaucoup de valeur, mais elle doit être transparente et responsable afin de protéger la vie privée des Canadiens et l'intégrité de la démocratie canadienne. Il faudra pour cela mettre à jour les lois sur la protection des renseignements personnels et les appliquer aux partis politiques, accroître les pouvoirs du Commissariat à la protection de la vie privée et tenir les plateformes responsables du contenu qu'elles choisissent d'autoriser et des raisons pour lesquelles elles l'autorisent.

Merci.

● (1110)

Le président: Merci, madame Dubois.

Nous passons maintenant la parole à Michael Pal.

M. Michael Pal (professeur agrégé, Faculté de droit, section de common law, Université d'Ottawa, à titre personnel): Merci beaucoup de m'avoir invité aujourd'hui.

Je suis professeur agrégé à la faculté de droit de l'Université d'Ottawa, où j'enseigne le droit électoral et le droit constitutionnel. J'y dirige aussi le groupe de droit public, mais aujourd'hui je vais vous présenter mes opinions personnelles. Je m'intéresse à des enjeux comme la protection des renseignements personnels des électeurs, les lois sur le financement des campagnes électorales comme elles s'appliquent en ligne et la réglementation des plateformes de médias sociaux ainsi que de la cybersécurité électorale. Aujourd'hui, j'aimerais vous parler un peu des partis politiques — et je sais que vous avez beaucoup entendu parler —, de la réglementation des plateformes de médias sociaux. Je parlerai ensuite de la cybersécurité, mais brièvement, puisque les derniers témoins ont déjà traité de ce sujet.

J'ai eu l'occasion de présenter certains de ces documents à vos collègues du Comité de la procédure et des affaires de la Chambre dans le cadre de leur étude du projet de loi C-76. J'ai donc aussi quelques commentaires à faire à ce sujet.

Le premier problème, que des témoins ont déjà présenté, est celui de la protection des renseignements personnels des électeurs par les partis politiques. Comme ma collègue, la professeure Dubois, l'a mentionné, les partis politiques sont l'une des rares grandes institutions et entités canadiennes qui ne soient pas assujetties à une réglementation stricte sur la protection de la vie privée. La Loi sur la protection des renseignements personnels ne les considère pas comme des entités gouvernementales, et ils ne se livrent pas à des activités commerciales en vertu de la LPRPDE. Ils se trouvent dans un vide juridique entre les deux grandes lois fédérales sur la protection des renseignements personnels.

Tout récemment, tous les commissaires à la protection de la vie privée du Canada — la commissaire fédérale et les commissaires provinciaux — ont déclaré que la situation était insatisfaisante et qu'il fallait la corriger. Seule la Colombie-Britannique assujettit les partis politiques aux lois provinciales sur la protection des renseignements personnels. Un projet de loi a été déposé au Québec, comme vous le savez, mais il n'a pas été adopté avant les élections qui viennent d'avoir lieu.

Le projet de loi C-76 prévoirait ces exigences dans une certaine mesure. Essentiellement, cependant, il exigerait que les partis suivent des politiques sur la protection de la vie privée et établissent des règles sur les enjeux particuliers que les politiques doivent aborder. Tous les grands partis inscrits ont déjà des politiques de confidentialité. Ce projet de loi pourrait changer certains des enjeux que ces politiques visent, parce que tous les partis n'abordent pas les mêmes enjeux, mais il ne donnerait pas clairement un pouvoir de surveillance au commissaire fédéral à la protection de la vie privée ou à Élections Canada. Il ne fixerait pas un contenu précis à insérer dans les politiques sur la protection de la vie privée. Il ne prévoit pas de mécanisme d'application de la loi. Donc à mon avis, c'est un bon début. C'est la mesure la plus importante que l'on ait prise pour exiger que les partis politiques protègent la vie privée, mais ce projet de loi ne va pas assez loin.

À quoi ressemblerait la réglementation des partis politiques pour protéger la vie privée des électeurs? On devrait révéler aux électeurs les données que les partis politiques détiennent à leur sujet. Les électeurs devraient avoir le droit de corriger les renseignements inexacts, ce qui est assez courant dans d'autres régimes de protection de la vie privée. Les électeurs devraient avoir l'assurance que les partis politiques ne devront utiliser les données qu'ils recueillent qu'à des fins politiques légitimes. Comme Mme Dubois l'a suggéré, il est bon que les partis politiques recueillent des renseignements sur les électeurs. Ils savent ainsi ce que ceux-ci désirent vraiment et ils apprennent à les connaître. Toutefois, ces données ne devraient être utilisées qu'à des fins politiques, à des fins électorales.

Je pense que certaines règles générales destinées à protéger la vie privée ne fonctionneraient pas dans ce cas, par exemple, la règle sur la liste de numéros de téléphone exclus. Les partis politiques doivent pouvoir communiquer avec les électeurs, et je pense qu'une telle liste nuirait à l'intégrité démocratique des élections si les partis politiques étaient incapables de communiquer avec 25, 30 ou 40 % des électeurs. À mon avis, il faudra adapter le contenu des règles en vigueur au contexte particulier des partis politiques et des élections.

La deuxième grande question que je voulais aborder est celle de la réglementation des plateformes de médias sociaux. Je sais que les témoins ont beaucoup parlé de Facebook. Une bonne partie de ce que je vais dire se trouve dans un document que j'ai remis récemment au MIT et que je serais heureux de fournir au Comité s'il le trouve utile. Comme vous le savez, la Loi électorale du Canada et les lois connexes régissent les partis politiques, les candidats à la direction, les candidats à l'investiture et les partis tiers. Il faudrait ajouter les plateformes de médias sociaux et les entreprises de technologie aux groupes qui sont explicitement réglementés par la Loi électorale du Canada et par les lois qui relèvent de ce comité. De quelle façon? Les plateformes devraient être responsables de divulguer et de tenir des dossiers sur la source de toute entité qui cherche à y afficher sa publicité.

Le projet de loi C-76 contient des mesures positives. Par exemple, il empêcherait Facebook d'accepter une publicité politique étrangère qui vise à influencer une élection canadienne. C'est un pas dans la bonne direction. Cette exigence ne s'appliquerait que pendant les campagnes électorales, si je l'ai bien comprise, et j'aimerais que l'on ajoute une règle plus robuste exigeant la diligence raisonnable des entreprises de médias sociaux. Ce contenu vient-il d'une personne réelle? Où se trouve cette personne? Essaie-t-elle de payer en roubles ou en dollars? A-t-elle fourni une adresse et les autres renseignements de base que logiquement, nous exigerions tous pour découvrir la source d'un don?

● (1115)

Tout cela a trait à l'ingérence étrangère. Ces mesures viseraient aussi à établir un système de financement des campagnes nationales intègre, compte tenu de toute la publicité qui se fait en ligne.

Une autre question qui, à mon avis, nécessite une réglementation plus poussée est celle des termes de recherche. On peut microcibler, par des annonces publicitaires, des utilisateurs particuliers d'une plateforme de médias sociaux. Si l'on diffuse une publicité électorale pendant La Soirée du hockey, nous pouvons voir le contenu de la publicité. En tant que membres du public, nous n'avons pas nécessairement l'occasion de voir une publicité qui vise une personne ou un groupe de personnes, et ces personnes ne savent peut-être même pas pourquoi on les a ciblées.

Selon moi, certains types de recherche n'ont pas leur place en politique électorale. Par exemple, on peut effectuer une recherche pour trouver des racistes, c'est possible, et il y a eu beaucoup de discussions dans les médias à ce sujet et à savoir si cela s'est produit lors de la dernière élection aux États-Unis. Je ne pense pas que nous ayons des renseignements concrets sur des cas particuliers, mais nous savons tous que les termes de recherche peuvent être utilisés d'une manière que nous jugeons répréhensible, en termes très vagues, sur la façon dont la démocratie devrait fonctionner au Canada.

Le public a donc intérêt à ce qu'on divulgue non seulement les termes de recherche, mais aussi les personnes qui ont été ciblées et qui ne savent peut-être pas pourquoi.

Il serait également bon de créer un dépôt public de toutes les publicités liées aux élections. Facebook l'a fait volontairement, mais cette décision pourrait être annulée à n'importe quel moment par des gens assis dans des bureaux en Californie. À mon avis, cette situation est inacceptable. Ce dépôt devrait être exigé par la loi.

Un précédent très intéressant a été soulevé au sujet de la communication politique sur WhatsApp. On parle encore moins de ce qui est envoyé par messagerie texte, surtout dans les applications de bout en bout chiffrées comme WhatsApp. Les médias ont révélé récemment que, lors des élections provinciales de l'Ontario, quelqu'un avait envoyé des communications politiques sur Xbox. Je n'utilise pas Xbox. Je ne joue pas à beaucoup de jeux vidéo, mais ceux qui y jouent peuvent être ciblés et recevoir des publicités électorales. Le public n'a aucun moyen de voir le contenu de ces publicités. J'aimerais donc que l'on divulgue constamment — et pas seulement pendant les campagnes — les publicités électorales affichées sur toutes les plateformes pertinentes.

Il faudrait aussi décider si les plateformes de médias sociaux devraient être traitées comme des diffuseurs. Je ne suis pas un expert en droit des télécommunications. Je ne prétends pas que Facebook devrait être considéré en tout temps comme un diffuseur à l'instar des chaînes CTV ou CBC. Cependant, la Loi électorale du Canada contient des dispositions sur les diffuseurs, notamment à l'article 348, qui exige que les radiodiffuseurs facturent le tarif le plus bas possible aux partis politiques qui désirent placer de la publicité sur leur plateforme. Cet article ouvre aux partis politiques l'accès aux réseaux de radio et de télédiffusion. Il veille aussi à ce que les tarifs soient sensiblement les mêmes. Il empêche les responsables de CTV, par exemple, d'offrir des tarifs préférentiels aux partis qu'ils préfèrent.

L'algorithme de vente aux enchères pour afficher de la publicité dans Facebook risque d'accroître considérablement la variation et les prix que les annonceurs devraient payer pour atteindre exactement le même public. À mon avis, cette approche est néfaste, car elle risque de faire pencher la balance dans une direction ou une autre.

Nous nous heurtons aussi à une « boîte noire » dans le cas des enchères publicitaires. Facebook n'indique pas exactement comment elles fonctionnent, parce que cette information est confidentielle, mais d'après ce que nous savons, il semblerait bien que l'article 348 les réglemente, même si nous ne considérons pas généralement Facebook comme un diffuseur.

Mon avant-dernière observation concerne la responsabilité. Pour que les plateformes de médias sociaux respectent les lois en vigueur, il faut leur en imposer la responsabilité. Elles ne sont généralement pas responsables du contenu qu'elles affichent, alors il me semble que ce comité et la Chambre en général devraient se pencher sur la possibilité de les rendre responsables de leurs violations répétées des normes électorales. À mon avis, il serait important d'examiner cette question importante.

Ma dernière observation concerne la cybersécurité électorale, car je crois comprendre que cet enjeu intéresse le Comité. La cybersécurité coûte cher. Je crois, par exemple, que les banques canadiennes dépensent beaucoup d'argent pour assurer la cybersécurité. Cela s'avérerait difficile pour les partis ou les entités politiques qui sont en pleine campagne électorale. Les partis politiques reçoivent des subventions gouvernementales indirectes par le système de remboursement, par exemple, des dépenses électorales. Il serait peut-être bon d'encourager les dépenses en cybersécurité en leur remboursant une partie de ces coûts. C'est une idée que j'essaie fortement de promouvoir depuis quelque temps.

● (1120)

Enfin, les États-Unis ont établi des protocoles très détaillés sur ce qui devrait se passer entre les organismes gouvernementaux en cas de cyberattaque, ce qui serait catastrophique en plein milieu de la campagne d'octobre 2019, par exemple. Quels seraient les protocoles? Élections Canada ou la nouvelle agence de cybersécurité mènent peut-être des discussions dont je ne suis pas au courant. J'espère qu'on en discute. Il est crucial que le public puisse se fier aux procédures suivies, parce que s'il ne les connaît pas, il risque de penser qu'un organisme favorise l'un des partis ou qu'un pays étranger s'ingère dans la campagne électorale au nom d'un parti ou d'un ensemble d'entités. Cela me semble assez évident après ce qui s'est passé aux États-Unis.

À mon avis, il serait bon de divulguer ces protocoles au public.

Merci beaucoup de votre attention. Je me ferai un grand plaisir de répondre à vos questions dans l'une ou l'autre des langues officielles.

Le président: Merci, monsieur Pal.

Enfin, nous entendrons Samantha Bradshaw par téléconférence.

À vous la parole. Vous avez 10 minutes.

Mme Samantha Bradshaw (chercheuse, à titre personnel): Excellent.

Merci de m'avoir invitée aujourd'hui.

Je m'appelle Samantha Bradshaw. Je participe au projet de recherche sur la propagande numérique à l'Université d'Oxford. Je vais abréger cela en appelant ce projet Comprop.

Dans le cadre de ce projet, nous étudions les incidences qu'ont les algorithmes, les mégadonnées et l'automatisation sur divers aspects de la vie publique. Nous nous efforçons d'étudier les problèmes que causent les informations bidon, la désinformation, les publicités politiques ciblées, les activités d'influence étrangère, les bulles filtres, les chambres d'écho. Autrement dit, nous étudions tous les graves problèmes liés aux médias sociaux et à la démocratie afin que le public les comprenne mieux et que nous puissions en discuter.

Aujourd'hui, je vais consacrer mes 10 minutes à certaines des études de recherche pertinentes qui, je crois, contribueront à éclairer les décisions que le Comité désire prendre.

L'un de nos grands volets de recherche porte sur la surveillance des élections et sur le genre de renseignements que les gens échangent avant de voter. Nous essayons d'évaluer la propagation de ce que nous appelons les « nouvelles au rabais ». Il ne s'agit pas seulement de fausses nouvelles et de renseignements trompeurs. Leur contenu est très polarisant — les discours haineux, le racisme, le sexisme —, ce sont des commentaires extrêmement partisans déguisés en nouvelle. C'est le genre de renseignements bidon que nous suivons pendant les campagnes électorales. Nous avons observé aux États-Unis les exemples les plus frappants de la diffusion d'informations bidon entourant les élections. Nous avons constaté un rapport de 1:1 entre la diffusion d'informations bidon et celle d'informations produites par des professionnels.

Le plus intéressant est la répartition de cette diffusion. On constate qu'elle a tendance à cibler les États indécis et les circonscriptions où 10 ou 15 votes pourraient faire pencher la balance de l'élection. Elle est vraiment importante, parce que le contenu ne se propage pas seulement de façon naturelle; il est souvent très ciblé. On trouve même des campagnes organisées de manière à influencer les électeurs dont le vote peut faire virer une élection d'un côté ou de l'autre.

Le deuxième élément de notre recherche que j'aimerais souligner ici concerne ce que nous appelons les « cybertroupes ». Ce sont des campagnes organisées dans le but de manipuler l'opinion publique. On confie ce travail à des employés d'organismes gouvernementaux, de partis politiques ou d'entités privées qui reçoivent un salaire et des avantages sociaux. Ils travaillent dans des salles climatisées et, dans le cadre de leurs fonctions, ils mènent des activités d'influence de l'opinion publique. Depuis deux ans, nous effectuons un inventaire global annuel pour estimer la capacité qu'ont divers gouvernements et acteurs de partis politiques à mener ces campagnes de manipulation dans les médias sociaux.

Nous avons fait quelques constatations intéressantes. Je ne vais pas tout décrire, parce que ce serait trop long, mais je vais souligner ce qui se passe dans les démocraties et décrire les principales menaces. Dans les démocraties, les partis politiques utilisent souvent des technologies comme les robots politiques pour amplifier des messages. Nous en avons même vu certains diffuser de la désinformation. Ces gouvernements utilisent aussi des tactiques de manipulation organisée contre leur propre population.

Bien des démocraties utilisent ces techniques psychologiques pour promouvoir leurs opérations militaires. Dans la plupart des cas, les partis politiques se concentrent sur la population de leur pays. Beaucoup d'acteurs privés participent aussi à ce genre d'activités pendant les campagnes électorales. Bien qu'un grand nombre de techniques de manipulation des médias sociaux aient été mises au point en 2009 ou 2010 dans des contextes plus militaires aux fins d'une guerre de l'information, à l'heure actuelle ces services sont fournis par des entreprises ou par des sociétés privées. Le meilleur exemple est celui de la société Cambridge Analytica, mais les diverses entreprises qui collaborent avec des politiciens ou avec des gouvernements pour manipuler les discussions publiques en ligne sont maintenant tellement nombreuses que ces pratiques deviennent nocives pour la démocratie et pour le débat démocratique.

● (1125)

En examinant ces problèmes, je trouve que le plus grand défi réside dans le fait que la majeure partie des données qui servent au ciblage ne viennent plus du gouvernement, de Statistique Canada, qui produit la meilleure information sur la vie publique canadienne. Elles viennent de sociétés privées comme Facebook et Google, qui recueillent des renseignements personnels et qui s'en servent pour cibler les gens pendant les campagnes électorales.

Auparavant, nous étions seulement les cibles de manipulations commerciales visant à vendre du shampooing ou d'autres types de produits. Nous en étions conscients et nous le tolérions. Mais maintenant, on essaie de nous vendre des idéologies politiques et des dirigeants internationaux. À mon avis, il faut que nous prenions un peu de recul pour décider dans quelle mesure nous devrions accepter d'être ciblés dans notre rôle d'électeurs.

Je sais que beaucoup de lois à l'heure actuelle portent sur la transparence et cherchent à sélectionner les raisons pour lesquelles nous recevons certains messages. Cependant, j'irais plus loin en demandant si ces lois devraient même permettre qu'on me cible parce que je vote libéral ou même pour d'autres traits mineurs de ma personnalité.

Un des témoins a mentionné tout à l'heure que certains électeurs sont ciblés pour leur attitude raciste. À mon avis, il est grand temps que nous remettions en question cette tolérance au ciblage mené à des niveaux très profonds de notre personnalité.

Dans le cas des menaces que les manipulations affichées dans les médias sociaux, la désinformation et la publicité ciblée nous posent, les contrefaçons complexes et l'intelligence artificielle perfectionnent tellement les robots politiques que l'on se demande de plus en plus si la personne qui a créé le compte ou qui anime le bot est humaine et plus réelle. Il devient donc toujours plus difficile pour les citoyens — et aussi pour les plateformes — de détecter les faux comptes qui diffusent de la désinformation pendant les campagnes électorales. C'est l'une des menaces qui se profilent à l'horizon.

Mme Dubois a parlé de plateformes de messagerie, de logiciels comme WhatsApp et Telegram. Bon nombre de ces chaînes cryptées sont incroyablement difficiles à étudier à cause de leur encodage. Il est évident que l'encodage est extrêmement important et que ces plateformes de communication sont très utiles. Toutefois, les torts qu'elles causent à la démocratie en diffusant de l'information au rabais soulèvent de graves questions auxquelles nous devons nous attaquer, surtout dans des pays comme l'Inde ou le Sri Lanka, où cette désinformation entraîne souvent la mort.

Le troisième élément à surveiller est la réglementation. Je perçois un risque réel de réglementation excessive dans ce domaine. En Europe, par exemple, notamment par la loi allemande sur les NetzDG, on a mis sur pied d'excellentes premières mesures pour améliorer la situation en imposant des amendes aux plateformes. J'imagine que cette loi a eu des conséquences imprévues, et je crois que nous en voyons toujours plus.

Je vais vous en citer un bon exemple. Dès l'entrée en vigueur de cette loi, une personne du parti de droite a affiché des commentaires horriblement racistes en ligne. On les a retirés, et c'est très bien, mais on a aussi retiré tous les commentaires politiques des gens qui qualifiaient ce commentaire de raciste. Par conséquent, en forçant les entreprises de médias sociaux à choisir elles-mêmes le contenu à afficher, on perd une partie très importante du débat démocratique.

À mon avis, la réglementation excessive est une menace et un défi à surveiller. Les gouvernements devront trouver moyen d'établir des règlements intelligents qui visent la cause même des problèmes au lieu de s'attaquer seulement à certains symptômes, comme le mauvais contenu.

Je vais m'arrêter ici. Je serai heureuse de répondre à vos questions.

● (1130)

Le président: Merci beaucoup, madame Bradshaw.

Monsieur Saini, vous avez 10 minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Merci à vous trois d'être ici aujourd'hui.

Madame Dubois, je vais commencer par vous parce que j'ai lu un article que vous avez écrit avec M. McKelvey, qui a comparu devant nous la semaine dernière. Vous y décrivez les quatre types de robots politiques. Une partie de cet article portait sur l'usage des robots politiques pour amplifier ou affaiblir des messages.

Ce qui m'inquiète, c'est qu'on crée ainsi des profils psychographiques des gens. On cible certaines personnes. On récolte des renseignements. Je m'inquiète de l'effet d'affaiblissement que peuvent avoir ces robots sur les renseignements recueillis. Cela risque-t-il de devenir une tactique pour empêcher les électeurs de voter?

Mme Elizabeth Dubois: Oui.

Dans l'étude que Fenwick McKelvey et moi-même avons menée sur les robots politiques, nous avons découvert que ces deux types de robots, ceux qui amplifient et ceux qui affaiblissent les messages, sont le plus souvent utilisés pour influencer négativement la diffusion de l'information politique.

Nous nous inquiétions entre autres de la suppression du droit de vote, parce que si le message « N'oubliez pas d'aller voter » cible un groupe particulièrement sous-représenté dans la sphère électorale canadienne — nous savons que les Néo-Canadiens ont des taux de participation électorale inférieurs à ceux des gens qui vivent ici depuis toujours —, et si quelqu'un amplifie le message qui tente de les dissuader de voter ou affaiblit le message qui vise à les encourager à voter, on risque injustement de les dissuader de participer aux élections.

Il existe d'autres stratégies secrètes semblables au scandale des appels automatisés, où quelqu'un a créé un message téléphonique automatisé qui dirigeait les électeurs vers le mauvais bureau de scrutin. Vous pouvez imaginer une version automatisée de cela sur Twitter ou sur WhatsApp, avec des scripts automatisés, ce qui représente essentiellement ce que nous vous décrivons en parlant de robots politiques.

● (1135)

M. Raj Saini: Vous écrivez dans cet article que vous préféreriez que l'on inscrive les robots politiques dans un registre plutôt que de les interdire.

Pensez-vous qu'il devrait y avoir une façon de déterminer si un bot est humain, afin que nous puissions l'inscrire en lui attribuant un identificateur quelconque pour que les gens sachent s'ils sont ciblés par un humain ou par un bot? Pensez-vous que ce serait utile?

Mme Elizabeth Dubois: Oui.

Je pense qu'il y a deux éléments importants. Quand je disais que nous devrions inscrire les robots, je parlais précisément de ceux qui sont utilisés pour communiquer avec les électeurs; de même, le registre de communication avec les électeurs ne doit pas servir à enregistrer toutes les communications qu'un parti politique échange avec chaque personne. Le registre de communication avec les électeurs pourrait servir à inscrire les comptes automatisés qui ciblent des gens pour les envoyer au mauvais bureau de scrutin.

M. Raj Saini: Puisque certains robots créent de la désinformation, qu'il s'agisse de renseignements racistes ou menaçants ou de quoi que ce soit du genre, pensez-vous que les entreprises de médias sociaux ont actuellement un mécanisme en place pour les éliminer le plus rapidement possible?

Mme Elizabeth Dubois: Oui.

C'est là que les choses se corsent. Si Twitter, par exemple, voulait éliminer dès maintenant toute automatisation de son compte, il pourrait le faire, mais ce ne serait pas très utile dans l'ensemble, parce que les gens profitent beaucoup de certains types de robots.

Pensez à tous les médias que vous voyez sur Twitter. Presque tous utilisent l'automatisation dans une certaine mesure dans leurs comptes Twitter pour diffuser simultanément des articles dans Twitter, Facebook et Instagram. C'est une forme de bot dans Twitter, alors je ne pense pas qu'il serait idéal d'éliminer toute l'automatisation.

Il y a aussi le problème des comptes Cyborg. Ces comptes sont parfois automatisés, mais d'autres fois un humain intervient et publie lui-même du contenu, littéralement en le tapant et en appuyant sur la touche Envoyer.

M. Raj Saini: Madame Bradshaw, vous avez beaucoup écrit sur la manipulation des médias sociaux et vous avez aussi parlé d'algorithmes.

À l'heure actuelle, nous assistons à la militarisation de ces algorithmes. Le but était de permettre aux gens de personnaliser leur contenu, mais maintenant, on les utilise pour faire de la désinformation. Pour contrer cela, les entreprises de médias sociaux ont suggéré que l'on crée un algorithme distinct pour contrôler les algorithmes qu'elles utilisent. Dans quelle mesure est-ce faisable?

Mme Samantha Bradshaw: Je pense qu'il est vraiment important d'avoir un élément humain qui examine et qui audite les algorithmes. On ne peut pas lancer de la poussière d'intelligence artificielle magique pour résoudre ce problème.

Cette technologie est excellente pour appuyer les décisions humaines, et c'est là que je vois beaucoup d'avantages à créer un deuxième algorithme, mais nous avons quand même besoin que les humains en revoient ensuite le contenu. Il y a tellement de décisions nuancées que ces algorithmes peuvent ou ne peuvent pas prendre, alors le jugement humain est vraiment important.

M. Raj Saini: Ma dernière question s'adresse à vous. Disons que pendant une campagne électorale, certaines entités, comme un parti tiers ou des entités politiques, conçoivent un algorithme pour cibler un certain type d'électeurs. Pensez-vous qu'il faudrait conserver ces algorithmes dans un dépôt afin que le lendemain, s'il y a des conséquences, comme vous le dites, des humains puissent analyser cet algorithme pour voir s'il a transmis de la désinformation ou un quelconque message utilisé de façon négative — je ne veux pas utiliser le mot « illégal » — de manière inconvenante pour cibler des électeurs particuliers? Des humains pourraient alors examiner cet algorithme pour déterminer s'il a été utilisé de façon négative.

● (1140)

Mme Samantha Bradshaw: Oui, je pense que ce serait logique. Il y a toujours un risque de rendre les algorithmes trop publics, cependant, parce que dès qu'ils deviennent très publics et qu'ils sont divulgués ouvertement, toute une industrie se précipite pour essayer de les décoder. Il est possible d'optimiser les moteurs de recherche, alors il ne faut pas rendre l'algorithme si transparent qu'on pourra facilement le manipuler.

M. Raj Saini: Madame Dubois, avez-vous quelque chose à dire à ce sujet?

Mme Elizabeth Dubois: Oui, je pense que la capacité de manipuler les algorithmes est un facteur à soupeser lorsqu'on crée un algorithme pour résoudre un problème avec l'intention de l'offrir ensuite à tout le monde. Je pense que cette transparence est importante, mais nous devons aussi publier des tests sur le fonctionnement des algorithmes, ce qui nous permettrait de vérifier et d'auditer ces systèmes sans nécessairement en ouvrir l'accès aux gens qui voudraient décoder l'algorithme.

Je pense que certaines des choses que j'ai dites dans ma déclaration préliminaire sont liées à cela. Il serait bon de créer un historique des décisions que l'équipe a prises en élaborant l'algorithme. On apprendra alors ce que l'algorithme était censé faire, pourquoi et comment. Voilà le genre d'information qui pourrait nous aider à résoudre le problème que vous soulignez d'une façon qui n'incite pas les gens à simplement tout décoder.

Le président: Merci.

C'est maintenant au tour de M. Kent, qui a sept minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président.

Je vous remercie tous de vos observations, de vos opinions et des conseils que vous avez fournis au Comité aujourd'hui.

Dans les 24 ou 35 heures qui se sont écoulées depuis que l'ALENA est devenu l'AEUMC, on n'a pas beaucoup parlé de la protection de la propriété intellectuelle et de l'univers numérique sans frontières. Mais on a entendu plusieurs personnes dire, ou lancer la rumeur selon laquelle la protection de la propriété intellectuelle canadienne relèvera désormais du régime américain, l'Amérique du Nord adoptera plus ou moins le système américain de protection de la propriété intellectuelle.

Certains laissent entendre qu'en fait, les grandes entreprises de technologie ne seront pas responsables du contenu de leurs plateformes, ce qui signifierait — on l'a laissé entendre, et j'aimerais savoir ce que vous en pensez tous les trois — qu'il ne serait pas possible d'enquêter sur le scandale Cambridge Analytica-AggregateIQ-Facebook, ou que ces sociétés ne seraient pas tenues de rendre des comptes sur le contenu de leurs plateformes et sur l'utilisation qu'on en fait.

Pourrions-nous commencer par vous, monsieur Pal?

M. Michael Pal: Merci beaucoup. Je pense que c'est une question importante.

Comme vous le dites, cela ne fait que 24 à 36 heures. J'ai eu l'occasion ce matin de jeter un coup d'oeil à l'article 19 qui, je crois, régit le commerce numérique ou la politique numérique. On y trouve deux ou trois choses pertinentes.

Premièrement, il semble — et j'oublie le terme exact utilisé dans l'article 19 — qu'essentiellement, en vertu de cet accord, les entreprises Internet, les plateformes de médias sociaux, ne seront pas responsables du contenu que l'on affichera sur leurs plateformes. Maintenant, il faudra insérer cela dans les lois nationales. En outre, le gouvernement fédéral et les provinces disposent d'une certaine marge de manoeuvre. On se heurtera à toutes sortes de problèmes, mais on trouve cela dans l'article 19.

Il y a aussi une disposition sur le code source qui mentionne les algorithmes. Mes collègues me corrigeront peut-être, mais si j'ai bien lu, elle inclut les algorithmes.

L'hon. Peter Kent: Je pense qu'il y a un point précis qui dit que les gouvernements ne pourront pas examiner les codes sources.

M. Michael Pal: Nous ne pourrions pas avoir une transparence algorithmique obligatoire, mais il y a une exception pour les enquêtes criminelles. Une enquête menée par Élections Canada ou le commissaire à la protection de la vie privée serait-elle considérée comme une enquête criminelle? Voilà le genre de question ouverte qui nous préoccupe.

Je n'ai pas d'opinion définitive sur l'article 19. Je n'en ai pris connaissance que ce matin. Je vais me montrer légaliste et faire preuve de prudence et je vais dire que je ne suis pas certain de toutes les conséquences qu'il entraîne. Il s'attaque au problème et semble le restreindre, à certains égards. J'ai parlé de la responsabilité des plateformes de médias sociaux pour le non-respect à répétition des normes au sujet des élections. L'article 19 de l'AEUMC pourrait avoir des répercussions qui rendraient cette proposition moins viable.

● (1145)

Mme Samantha Bradshaw: Comme vous l'avez mentionné, c'est assez nouveau. Je n'ai pas encore vu le document. Je sais que les plateformes de médias sociaux ont toujours bénéficié de dispositions d'exonération qui les protègent contre le contenu que les gens affichent. À l'époque, nous considérions que c'était une bonne chose parce que nous ne voulions pas tenir Google responsable du téléchargement de contenu par quelqu'un d'autre. Google Search ne fonctionnerait pas, ou n'existerait pas aujourd'hui, si Google devait être responsable de l'organisation de certains types de renseignements illégaux.

Pour ce qui est de tenir Facebook responsable de Cambridge Analytica, je ne suis pas tout à fait sûre des répercussions de ce nouvel accord, mais je pense que c'est une question très importante. Je suis désolée de ne pas être plus au courant.

L'hon. Peter Kent: Merci.

Madame Dubois.

Mme Elizabeth Dubois: Merci.

Je n'ai pas moi non plus encore pris connaissance des détails de l'AEUMC, mais j'estime que les questions soulevées sont importantes et que nous devons les examiner.

Pour enchaîner sur ce que Mme Bradshaw vient de souligner, je dirais que l'idée que les plateformes soient responsables de tout le contenu qui s'y trouve est une question importante. Comme elle l'a indiqué, c'est un outil vraiment précieux pour la croissance de ces entreprises et pour l'innovation dans notre façon de gérer les tonnes de données et de renseignements qui existent maintenant et c'est utile. Cependant, je pense qu'il y a une distinction importante à faire entre permettre l'existence de ce contenu et en être responsable et être responsable de ce que le contenu fait apparaître comme des sujets tendance, des résultats de recherche recommandés ou de l'information qui figure en haut des fils de nouvelles des gens.

Il y a des décisions que ces plateformes prennent déjà au sujet de ce qui est mis en vedette et de ce qui ne l'est pas et ces décisions doivent être prises en se demandant si elles musellent ou non des groupes qui ne devraient pas être réduits au silence ou qui font la promotion de contenu raciste ou haineux qui ne devrait pas être promu et présenté.

Sans avoir examiné l'AEUMC, je ne peux pas dire si cette distinction entre le contenu et la diffusion du contenu a été abordée, ni quelles en sont les conséquences, mais je pense que c'est un point important qui doit être examiné.

L'hon. Peter Kent: Des discussions préliminaires semblent indiquer qu'il est possible que cela place l'Amérique du Nord et la protection de la vie privée en Amérique du Nord en contradiction avec le RGPD, par exemple, de sorte que le régime nord-américain irait à l'encontre de celui en vigueur certainement en Europe et de ceux en vigueur peut-être aussi dans d'autre pays.

Mme Elizabeth Dubois: Il semble que cela sera très dispendieux pour bien des entreprises et que ce sera problématique pour les citoyens si c'est le cas, mais je ne connais pas les détails.

L'hon. Peter Kent: Monsieur Pal, puis-je vous demander ce que vous pensez du RGPD, qui est entré en vigueur il y a moins de six mois, mais qui a déjà eu une incidence sur le comportement de certains organes de presse nord-américains — surtout américains — en les obligeant à se retirer du circuit de distribution en Europe par crainte de poursuites?

M. Michael Pal: Je pense que nous avons des leçons à tirer du RGPD. Je ne suis même pas certain que les experts européens en matière de protection de la vie privée comprennent vraiment comment cela va fonctionner dans la pratique. Qu'est-ce que cela signifie pour les organes de presse? Qu'est-ce que cela signifie pour les entreprises de technologie?

Je pense cependant que cela montre que beaucoup de ces entreprises de technologie ont leur siège social aux États-Unis ou à l'étranger, de sorte que, d'une certaine façon, chaque État national a perdu le contrôle d'une partie de la conversation au sujet des élections. Il n'y a pas que CTV, CBC et les autres radiodiffuseurs nationaux. Je pense qu'il incombe à chacun des États d'essayer de...

Nous ne devrions pas nous fier au RGPD, aux lois de la Californie ou aux lois fédérales américaines. Nous devons, nous les Canadiens, établir nos propres règles. Je pense que Mme Bradshaw a fait valoir un point important, à savoir que nous voulons faciliter l'expression politique et non la restreindre. Certaines des lois qui pourraient être adoptées pourraient restreindre l'expression politique. C'est un droit protégé par la Charte — l'alinéa 2b) — et nous ne voulons pas le restreindre.

Toutefois, les considérations relatives à la Charte sont amoindries dans le domaine de l'ingérence étrangère ou par des acteurs, des particuliers ou des entités étrangers qui expriment des opinions sur la politique canadienne. À mon avis, la réglementation des entreprises Internet ou de la protection des renseignements personnels des électeurs qui limite l'ingérence étrangère repose sur des motifs juridiques et théoriques prévus dans les lois et la Constitution beaucoup plus solides.

● (1150)

L'hon. Peter Kent: Y a-t-il du temps pour Mme Bradshaw?

Le président: Il n'y en a pas.

M. Michael Pal: Je ne critique pas Mme Bradshaw. Je pense qu'elle a soulevé un bon point à ce sujet, mais c'est l'implication constitutionnelle plus générale.

L'hon. Peter Kent: Nous pourrons peut-être y revenir plus tard.

Le président: Oui, bien sûr.

Merci, monsieur Kent.

C'est maintenant au tour de M. Angus, pour sept minutes.

M. Charlie Angus (Timmins—Baie James, NPD): Merci beaucoup.

Je veux parler de la décision du gouvernement de ne pas assujettir les partis politiques à la LPRPDE ou à un régime semblable qui tiendrait compte des différences entre les partis politiques et les entités commerciales. Si vous parlez aux membres de notre comité, vous constaterez que cela nous préoccupe beaucoup, parce que nous nous sommes penchés sur la capacité des tierces parties de miner les démocraties. Si vous parlez à nos organisateurs politiques, vous verrez qu'ils sont absolument enchantés, car nous sommes maintenant dans une course aux armements numériques et qu'aucun parti politique ne sera prêt à déposer les armes en premier parce qu'il voit la possibilité de faire de plus en plus de ciblage, de devenir de plus en plus précis et de déplacer les votes dans des domaines clés. C'est la réalité à laquelle nous sommes confrontés et le monde est complètement différent de ce qu'il était en 2015 pour ce qui est du rythme auquel les choses évoluent.

Monsieur Pal, j'aimerais vous poser une question sur l'importance de mettre en place certaines dispositions pour éviter de rater la cible avec ces armes, parce que nous avons vu ce qui s'est passé aux États-Unis et nous avons vu comment le vote sur le Brexit peut être manipulé. Pensez-vous que nous avons besoin d'un régime législatif solide et à quoi ressemblerait une certaine forme de reddition de comptes quant à la façon dont nos partis et d'autres intervenants utilisent cette information sur le plan politique?

M. Michael Pal: Vous avez tout à fait raison de dire que le scénario de 2019 est très différent de celui de 2015. Les choses évoluent très rapidement, et le risque, c'est que vous puissiez mettre en place un règlement trop intrusif ou qui n'a pas vraiment l'effet escompté ou les bonnes conséquences. J'en suis toujours conscient, mais je pense que nous avons une foule de bons renseignements. Les partis politiques recueillent d'énormes quantités de données, des données personnelles et des données de nature délicate. Les partis l'ont toujours fait, mais on arrive à un autre niveau. Pour moi, c'est une question non partisane. Cela ne touche pas un parti plus que l'autre, mais à l'heure actuelle, tous les acteurs politiques sont incités à améliorer leurs opérations de données et leur jeu de données.

Ce que j'essaie de dire, c'est que les règles sur la protection de la vie privée sont avantageuses pour les partis politiques. Personne ne veut être réglementé et cela peut sembler onéreux et coûter de l'argent, mais imaginez ce qui se passerait si l'un des principaux partis politiques du Canada était victime de piratage, un peu comme ce qui s'est passé avec le Parti démocratique aux États-Unis. Il ne faudrait pas beaucoup d'actes de piratage ou de cas de divulgation de renseignements personnels par, disons, un acteur étranger malveillant pour que le public perde confiance dans le parti politique ou l'ensemble du système. Je pense que nous sommes arrivés à un point où il est très important de régler les questions de protection de la vie privée et ce, dans l'intérêt des partis politiques en soi.

J'ai essayé de suggérer quelques éléments de contenu, comme le droit de savoir quelles données un parti politique détient à votre sujet et le droit de corriger des informations erronées. Les bénévoles, comme vous le savez tous, font beaucoup de travail et lorsque vous entrez de l'information sur une application ou sur un bout de papier, il est très possible que l'information soit inexacte et il se peut que l'électeur, la personne, ne le souhaite pas. Je pense qu'il pourrait également être utile de déterminer qui a accès aux bases de données des partis politiques ou, à tout le moins, d'en divulguer les coordonnées.

Je comprends que cela peut parfois sembler onéreux pour les partis politiques, mais je pense qu'ils contribuent grandement à inspirer confiance aux électeurs en leur montrant que les partis ont leurs intérêts à coeur. Un acte de piratage, c'est le pire des scénarios. Nous avons été témoins d'attaques de déni de service contre les partis politiques. Je crois que le premier ministre a résumé le rapport du Centre de la sécurité des télécommunications, selon lequel il y a eu des attaques de bas niveau lors des élections de 2015. Le CST a dit qu'il y avait eu plus de 40 incidents d'interférence dans le monde, alors nous ne devrions pas considérer le Canada comme un pays isolé. J'ai beaucoup de craintes pour les élections de 2019 et je pense que la protection de la vie privée en apaise certaines.

● (1155)

M. Charlie Angus: Madame Bradshaw, votre analyse des nouvelles simulées m'intéresse beaucoup. Vous parlez de « cybertroupes », d'opérations psychologiques et de militarisation de l'IA.

En 2015, dans ma région, parce que je vis essentiellement sur Facebook, selon ma femme, j'ai constaté quelque chose de complètement différent de ce qui était rapporté dans les médias nationaux. J'ai vu des publications profondément racistes, surtout en Grande-Bretagne, des commentaires anti-musulmans, des publications attaquant les immigrants et les réfugiés. Ils étaient très ciblés. Ils passaient par Facebook pour cibler des secteurs clés de ma région parmi des électeurs clés.

Le message véhiculé était complètement différent de ce qui se passait à l'échelle nationale. Cela n'a pas vraiment été remarqué, parce que nous prêtons toujours attention à ce que Peter Mansbridge dit à 18 heures.

J'ai toujours pensé qu'il fallait que le ciblage ait été meilleur ou plus clair pour que des utilisateurs de Facebook qui d'habitude ne se mêlent pas de politique se mettent soudainement à répéter ce genre de message. Cela semble être ce que nous avons constaté avec le Brexit, l'idée que des groupes comme Cambridge Analytica peuvent cibler précisément les électeurs des bureaux de scrutin, les électeurs qui vont en fait exercer une influence et ainsi de suite.

Vous avez parlé de la façon dont cela a été utilisé dans les États où les électeurs étaient indécis. J'aimerais que vous nous en disiez davantage à ce sujet.

J'aimerais aussi que vous nous en disiez davantage... parce que nous parlons sans cesse des tiers comme s'il s'agissait simplement de mauvais mercenaires. Vous avez parlé de ceux qui font de l'influence politique et qui se trouvent à l'intérieur des partis. Pouvez-vous nous parler des liens entre les membres des partis et ces agents tiers et nous expliquer comment ils utilisent cette désinformation en ligne?

Mme Samantha Bradshaw: Si nous regardons ce qui se passe aux États-Unis et les nouvelles simulées qui sont diffusées dans les États indécis, ça se limite à Twitter. Il ne s'agissait pas d'une analyse de Facebook, mais seulement de Twitter et de ce que les gens partageaient comme nouvelles et information.

Nous avons analysé quelques millions de gazouillis dans les 11 jours précédant le vote. Si vous regardez en moyenne les adresses URL que les utilisateurs partageaient dans les États indécis, vous constaterez qu'ils ont tendance à signaler des taux plus élevés de nouvelles et d'informations importunes, comparativement aux États incontestés. Par conséquent, c'est en partie à cause de la campagne de désinformation quelque peu organique. Cela ne se fait pas nécessairement par la publicité, mais l'information se propage naturellement sur les plateformes par les utilisateurs, ou peut-être par des robots, qui ont joué un rôle dans l'amplification de beaucoup de ces histoires.

Nous avons mesuré l'origine des comptes en utilisant des données géolocalisées. Si un utilisateur avait déclaré se trouver au Michigan, par exemple, l'un des États indécis, c'est ainsi que nous avons déterminé où se trouvait l'information et où se concentraient les nouvelles simulées.

Il y a le côté organique, mais il y a aussi celui de la publicité ciblée. Nous avons beaucoup d'informations sur la Russie, grâce aux révélations sur Facebook concernant des agents russes qui achètent des publicités politiques et les ciblent vers les électeurs en fonction de leur identité ou de leurs valeurs. Ils se sont ralliés à des groupes comme les défenseurs du droit du port d'armes à feu et le mouvement Black Lives Matter.

Ils avaient aussi tendance à jouer des deux côtés du spectre politique. Il ne s'agissait pas seulement d'appuyer Trump. Ils ont également appuyé des candidats comme Jill Stein et Bernie Sanders. En revanche, ils n'ont jamais appuyé Clinton. Ils l'attaquaient toujours publiquement.

Ce qui vient des partis politiques en soi est vraiment difficile à retracer. Cela nous ramène à la question que vous avez posée plus tôt au sujet des lois et de ce que nous pouvons faire pour mieux cibler.

Nous avons interviewé beaucoup de développeurs de robots qui ont oeuvré dans des campagnes pour divers partis. Ce sont eux qui ont créé les robots politiques pour amplifier certains messages. Il est difficile de retracer ce qu'ils ont fait pour un parti politique en raison de la loi sur le financement des campagnes électorales qui exige des rapports à deux niveaux seulement. En règle générale, ces contrats sont attribués à une grande entreprise de communications stratégiques, qui confie ensuite le travail à une entreprise spécialisée de Facebook, qui le confie ensuite à un groupe d'entrepreneurs indépendants. En déroulant la liste, vous arrivez au développeur de robots, que nous avons interviewé.

Nous n'avons pas de données précises sur les partis pour lesquels ces groupes ont travaillé, du moins aucune que je puisse partager en raison de nos ententes d'éthique avec ces développeurs. Le gros problème, c'est que nous sommes incapables de faire un suivi à cause des lois sur le financement des campagnes électorales.

● (1200)

Le président: Merci.

La parole est maintenant à M. Picard.

M. Michel Picard (Montarville, Lib.): Mon introduction sera peut-être longue, alors je vous demande d'être patients.

Dans mes commentaires, je ne tiendrai pas compte de la désinformation, par exemple, des appels pour envoyer un électeur au mauvais bureau de scrutin ou de toute autre chose visée par le Code criminel.

Lorsqu'on parlait de nouvelles simulées, de fausses nouvelles, peu importe, pendant la guerre froide et surtout en temps de guerre, la propagande était l'un des meilleurs outils en ville pour faire passer votre message, quel qu'il soit. Ceci et des magazines, des photos dans les pays du Moyen-Orient, où vous voyez de la nourriture, tout le monde à la table, de grandes voitures, des gens bien habillés, juste pour monter la population contre le gouvernement de son pays...

À l'époque, envoyer un millier de lettres pour faire de la publicité, peu importe, coûtait une fortune. Il fallait envoyer une ou deux pages. Aujourd'hui, vous envoyez de cinq à 10 millions de courriels en un clic — sans frais.

Je vais vous faire part de mon hypothèse et j'aimerais que vous y réfléchissiez; vous examinez le problème sous le mauvais angle. Nous essayons de nous concentrer sur ceux qui fournissent cette information et ce mauvais contenu et de réglementer les médias sociaux des entreprises car ce qu'ils font n'est pas bien, probablement parce que les gens sont trop paresseux pour contre-vérifier et vérifier l'information eux-mêmes. Soit dit en passant, nous n'empêchons pas les gens de voir des renseignements précis. Nous téléchargeons une énorme quantité d'information et on ne sait plus où on en est.

Dans l'optique de la réglementation, comment voulez-vous que le gouvernement agisse à l'égard des entreprises qui envoient ce genre de contenu sans toucher à leur liberté d'expression?

Mme Elizabeth Dubois: Je peux commencer.

Je comprends que vous voulez séparer les choses comme les tactiques de suppression des votes des nouvelles et du contenu bidon. Cependant, lorsque nous réfléchissons à la façon de régler l'un de ces problèmes et pas l'autre, il est très difficile de dire que nous allons réglementer seulement un aspect des plateformes et que nous aurons une solution complètement différente pour un autre. Les conversations vont de pair, parce que les mécanismes permettant de transmettre l'information à la première page du fil de nouvelles de quelqu'un sont les mêmes.

Il y a ce genre de défi technique, mais je pense qu'il importe vraiment de trouver un équilibre entre cela et les questions sur la liberté d'expression. Nous ne voulons pas d'une démocratie qui empêche des gens de partager leurs opinions ou qui les réduit au silence. Nul doute que c'est un problème.

Nous devons toutefois penser à l'évolution du système médiatique. Il faut tenir compte du fait qu'auparavant, cela coûtait beaucoup plus cher et prenait beaucoup plus de ressources pour répandre de la désinformation. Maintenant, il est très facile de le faire.

Nous savons aussi que les gens n'avaient pas beaucoup de choix quant au contenu qu'ils recevaient. Il était beaucoup plus simple pour eux de se familiariser avec les médias et de ne pas être paresseux, selon vos termes. Il y avait moins de vérifications à faire. Il y avait moins de travail à faire pour s'assurer de savoir quel contenu apparaissait et qui le créait. Les personnes qui pouvaient se permettre une licence de radiodiffusion étaient peu nombreuses.

Les attentes que nous imposons aux citoyens dans ce contexte sont très différentes de celles que nous leur imposons en leur disant que nous ne pouvons pas réglementer les plateformes et que c'est leur responsabilité. Dans l'environnement médiatique que nous avons, je pense qu'il est déraisonnable de s'attendre à ce que les citoyens puissent discerner les différentes sources de contenu, ce qui est vrai et ce qui ne l'est pas, sans un certain soutien.

Je ne veux pas laisser les citoyens s'en tirer à bon compte. Je pense que la littératie numérique et la littératie médiatique sont très importantes, mais je pense que ce n'est qu'une pièce du casse-tête.

M. Michel Picard: Quelqu'un d'autre...?

Mme Samantha Bradshaw: Il s'agit en grande partie de régler certains de ces grands problèmes systémiques entourant les plateformes. Si nous pouvions nous attaquer à la cause profonde des informations inutiles et de la diffusion si rapide de ces informations sur les plateformes de médias sociaux, nous pourrions aussi nous attaquer à ce problème tout en protégeant la liberté d'expression.

À mon avis, bon nombre des problèmes systémiques sont liés à l'économie de l'attention et à la façon dont, dans un monde où l'information est omniprésente, l'attention devient notre ressource rare. Les plateformes reposent sur cette économie de l'attention. Elles sont conçues pour adapter le contenu, l'information et la publicité à nos besoins, ce qui est le but de ces nouvelles au rabais. Les contenus sont des pièges à clics, conçus pour susciter nos émotions et nous mettre en colère ou nous rendre heureux, pour attirer notre attention.

Si nous pouvions commencer à examiner la façon dont les médias sociaux adaptent le contenu pour les utilisateurs en examinant les principes qui sous-tendent leur conception algorithmique — la pertinence et la viralité, par exemple, sont des éléments très importants dans les algorithmes actuels — et les remplacer par des principes qui appuieraient une meilleure démocratie, alors nous pourrions commencer à réglementer les plateformes de façon à ne pas nuire à la liberté d'expression.

● (1205)

M. Michael Pal: La réglementation des nouvelles bidon est la principale difficulté. Mes nouvelles bidon ne sont peut-être pas les mêmes que les vôtres. La suppression du vote est déjà illégale. L'ingérence étrangère est déjà illégale et le projet de loi C-76 contient d'excellentes mesures pour éliminer les dernières échappatoires. Le projet de loi C-76 érigerait en infraction le fait de se faire passer pour un politicien ou un parti politique, de sorte qu'il serait impossible de prétendre que la publicité provient d'un représentant ou d'un parti élu en particulier.

Dans la Loi électorale du Canada, il est déjà illégal, si vous êtes candidat, de prétendre que la personne contre laquelle vous vous présentez va abandonner la course pour une raison ou une autre. C'était une tactique courante et nous avons donc légiféré contre cette pratique. Dans le cas du projet de loi C-76, nous avons mis à jour la Loi pour tenir compte des nouveaux stratagèmes, quels qu'ils soient. Je ne vois pas de problème à dire: « Aujourd'hui, beaucoup de manoeuvres déloyales se produisent sur les médias sociaux. Quelles entités ont les ressources et la capacité de s'assurer que les règles sont respectées? »

Il est impossible de retracer tous les auteurs d'informations erronées, de désinformation et de suppression de votes. Il est beaucoup plus facile de réglementer les plateformes de médias sociaux. C'est réalisable sur le plan technologique. Ces médias nous révèlent qu'ils changent le monde. Ils devraient être en mesure de faire preuve de transparence et d'avoir accès à un répertoire de publicités électorales sans nuire aux résultats et je pense que nous pouvons le faire dans le respect de la liberté d'expression politique. L'une des choses que nous avons apprises au cours des 18 derniers mois, c'est qu'il faut réglementer les plateformes de médias sociaux.

Le président: Merci.

C'est maintenant au tour de M. Gourde pour cinq minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Je remercie les témoins d'être ici ce matin.

J'aimerais revenir à la racine du problème de la communication.

Nous, les candidats à une élection, devons rejoindre entre 90 000 et 110 000 électeurs dans une courte période de temps, soit environ deux mois. Nous, les députés, avons plus de temps parce que nous sommes déjà dans notre circonscription. Si on veut être équitable pour tout le monde, cette période est d'un maximum de deux mois.

Le défi est très grand car il est difficile de rejoindre les gens. L'information que nous fournit Élections Canada est l'adresse et le nom, point à la ligne.

Il y a deux façons de rejoindre les électeurs, et c'est le porte-à-porte et le numéro de téléphone, mais il y a de moins de moins de lignes de téléphone fixes. Il nous reste donc à trouver les numéros de téléphone cellulaire, ce qui est plus ou moins légal, car c'est considéré comme confidentiel, au Canada.

Le recours aux plateformes numériques est devenu un mal nécessaire pour l'ensemble des futurs politiciens, s'ils veulent rejoindre un grand nombre de personnes dans une période de temps très restreinte. Nous disposons de moins de 1 000 heures pour rejoindre 100 000 personnes, ce qui ne fait pas beaucoup de minutes par personne. C'est peut-être pour cela que le ciblage devient très intéressant pour les politiciens.

Pensez-vous qu'il serait possible de légiférer en matière de plateformes, afin de restreindre l'accès à certaines informations ou de donner plus d'accès aux politiciens à ces plateformes pour rejoindre les gens?

Si on ne peut pas obtenir les numéros de téléphone, on va sur les plateformes numériques. Si les politiciens avaient accès aux numéros de téléphone cellulaire, ils pourraient appeler les gens et discuter avec eux pour avoir à tout le moins un contact direct.

Présentement, on fait de la politique au moyen de contacts indirects. Pour rejoindre un électeur, on se fie à des machines et à une intelligence artificielle. Ce n'est pas l'essence de la démocratie. On ne fait pas élire des robots, mais des députés de partis politiques et un premier ministre.

Le temps dont nous disposons pour rejoindre les électeurs est très limité, et j'y vois un problème pour la démocratie à court, moyen et long terme. C'est la racine du problème. Tout le reste découle du problème lié au manque de temps et d'information.

Les numéros de téléphone de ligne fixe et de téléphone cellulaire devraient-ils être fournis par Élections Canada?

● (1210)

[*Traduction*]

M. Michael Pal: Une solution serait que les partis politiques disposent d'informations plus cohérentes. Comme vous l'avez dit, la Loi électorale fournit des renseignements de base sur le nom et l'adresse. Une option serait de fournir d'autres renseignements.

Vous avez suggéré des numéros de téléphone. Cela me met un peu mal à l'aise.

[*Français*]

Je ne pense pas que les gens aimeraient que les partis politiques aient leurs numéros de téléphone cellulaire.

[*Traduction*]

Il faudrait que j'y réfléchisse davantage. Si les partis politiques avaient le droit de divulguer plus d'informations sur les électeurs, il devrait y avoir une plus grande protection de la vie privée de ces renseignements. S'il s'agit d'une directive stratégique que le Comité envisage de recommander ou que vous le faites en tant que particulier, alors il doit y avoir un équilibre entre les protections accrues de la vie privée et l'information dont disposent les partis.

Pourrait-on faire le point sur les renseignements de base qui sont fournis? C'est une proposition intéressante que je n'avais jamais entendue auparavant.

Mme Elizabeth Dubois: Un problème potentiel lié à l'obligation d'enregistrer et de fournir un numéro de téléphone est qu'un grand nombre d'applications mobiles se connectent maintenant aux numéros de téléphone cellulaire des gens, ce qui signifie qu'en permettant ou en forçant la communication d'un numéro de téléphone, il pourrait y avoir des ramifications pour toutes sortes de regroupements de données, ce qui irait au-delà du principe... Un politicien ou un candidat devrait pouvoir communiquer directement avec ses électeurs et essayer de les faire participer au processus électoral, ce qui est très bien, à mon avis, mais je crains de créer une situation où les gens donnent sans le savoir aux candidats l'accès à toutes sortes de renseignements, des applications de rencontre à Facebook en passant par les listes d'Airbnb.

Ce n'est pas nécessairement que les listes précises vont se retrouver entre les mains d'un candidat, mais je pense que les possibilités de communication de données quand on utilise un numéro de téléphone cellulaire doivent faire l'objet d'une enquête. Je ne dis pas que c'est nécessairement une mauvaise idée, mais ce n'est pas une idée que j'avais envisagée auparavant. Ma réaction instinctive immédiate est que nous devons nous préoccuper de la façon dont les différents ensembles de données peuvent être reliés.

Je pense que votre argument fondamental selon lequel les candidats doivent être en mesure de communiquer avec les citoyens est important et, en particulier, les candidats qui ne sont pas titulaires se retrouvent désavantagés s'ils n'ont pas suffisamment de données pour établir ce contact de base.

Mme Samantha Bradshaw: Je vais intervenir pour le dernier point.

Je suis tout à fait d'accord avec Mme Dubois au sujet des dangers de pouvoir relier un numéro de téléphone, par exemple, à d'autres ensembles de données, parce que la plupart des gens relient leur numéro de téléphone cellulaire à leur profil Facebook et à d'autres plateformes de médias sociaux. Il y a un réel danger que vous commenciez à obtenir plus que le simple numéro de téléphone et les coordonnées de base.

Je pense que cela va au coeur de l'un des grands problèmes que nous voulons régler ici, c'est-à-dire que les partis politiques devraient être autorisés à utiliser ce genre de données lorsqu'ils font campagne et qu'ils s'adressent aux électeurs. Quelles sont les limites de ces données? Je pense qu'une fois que nous aurons trouvé de bonnes réponses à ces questions, que nous les appliquerons et que nous aurons créé plus de transparence à l'égard des données que les partis politiques ont entre eux et les électeurs, ce sera une victoire pour la démocratie.

● (1215)

Le président: Merci, monsieur Gourde.

La parole est maintenant à Mme Fortier.

[*Français*]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Merci beaucoup.

Je vous remercie tous les trois d'être là aujourd'hui. Nous travaillons très fort à cette étude et vous nous avez transmis des informations très pertinentes pour notre exercice.

Monsieur Pal, vous avez mentionné que le projet de loi C-76 présentait des mesures pour remédier à l'interférence étrangère et nationale dans les élections. Comment ces changements pourraient-ils avoir un effet en ce qui concerne les tiers partis? C'est l'une de mes préoccupations.

Lors de l'élection récente en Ontario, nous avons vu Ontario Proud, par exemple, promouvoir l'information d'un parti en particulier et pas celle des autres partis. Croyez-vous qu'une organisation comme celle-là pourrait être influencée par un tiers parti étranger ou par un gouvernement qui a de grandes quantités de données en sa possession?

Comment pouvons-nous limiter le partage de grandes quantités de données par des pays ayant moins de règlements, même s'il n'y a pas nécessairement d'échange financier?

Monsieur Pal, je vous laisse commencer, et les deux autres témoins pourront intervenir par la suite.

M. Michael Pal: Je vous remercie de votre question. Je vais y répondre en anglais pour être très précis.

[*Traduction*]

Le projet de loi C-76 comble l'une des lacunes qui existait encore en matière d'ingérence étrangère. Il était déjà illégal pour des entités étrangères de s'ingérer dans une élection canadienne, mais il y avait une échappatoire si vous dépensiez moins de 500 $. Cinq cents dollars peuvent en fait vous procurer beaucoup de publicités sur Facebook dans certains marchés. Cela éliminerait cette faille. C'est une mesure très importante.

Combien coûte l'envoi massif de messages WhatsApp ou la publicité sur Xbox? Je ne connais pas la réponse à cette question. Ce sont des utilisations émergentes. Mes collègues ont peut-être une idée des chiffres. Nous ne savons pas exactement quelle incidence cela aura sur les autres plateformes, mais je pense que cela aidera certainement pour ce qui est de la publicité sur Facebook ou Twitter.

Je crois que les tiers jouent un rôle de plus en plus important. Il y a eu une augmentation de tiers partis lors des dernières élections fédérales comparativement aux élections précédentes. Je pense qu'il est raisonnable de s'attendre à ce que cela continue. Les tiers ne sont essentiellement soumis à une réglementation stricte que pour ce qui est de leurs dépenses pendant la campagne électorale, ce qui est relativement court. De toute évidence, on peut essayer d'influencer les électeurs avant le début officiel de la campagne, ce que les partis politiques ont manifestement compris, mais aussi les tiers partis.

Dans le cadre de mes travaux universitaires, j'ai milité en faveur de la mise en oeuvre avant les élections... c'est-à-dire avant les règles officielles de la campagne électorale, dont certaines se trouvent dans le projet de loi C-76. Les limites de dépenses s'appliqueraient à ce qu'on appelle la « publicité partisane » pendant la période préélectorale. J'en suis très heureux. Je pense en fait que la période préélectorale devrait être plus longue. Je l'ai mentionné à vos collègues du comité de la procédure.

Mais nous avons une campagne permanente. Les tiers l'ont compris. Il y a d'autres administrations qui prennent des mesures encore plus fermes... Devrait-il y avoir divulgation de la publicité par des tiers pendant toute l'année précédant la date des élections à date fixe? Devrait-il y avoir des limites de dépenses? Je pense qu'il y a un très bon argument en faveur de cela.

[*Français*]

Mme Mona Fortier: J'aimerais laisser aux deux autres témoins le temps de répondre. Je vous remercie de nous avoir communiqué cela.

Par ailleurs, dans votre présentation, vous avez parlé d'une étude que vous avez présentée au MIT. Pourriez-vous la transmettre au Comité?

M. Michael Pal: Je le ferai avec plaisir, madame.

Mme Mona Fortier: Je vous remercie.

Madame Dubois, voulez-vous répondre à ma question?

Mme Elizabeth Dubois: Oui. Je vais aussi répondre en anglais,

[*Traduction*]

simplement pour être précise.

Je pense qu'un des principaux éléments s'ajoute à ce que M. Pal vient de dire au sujet de la campagne permanente et de la réglementation des tierces parties. En plus de la publicité et des dépenses, nous avons des questions au sujet de la collecte de données elle-même. Il ne s'agit pas seulement d'utiliser les données pour faire le ciblage, mais de recueillir les données au départ. Nous voyons fréquemment cette situation se produire en dehors de la période électorale.

Vous avez mentionné l'organisme Ontario Proud. Cette organisation est inscrite en tant que tiers parti établi, mais elle n'était pas sur pied depuis très longtemps quand elle recueillait déjà des utilisateurs sur Facebook et mettait à jour ses listes d'envoi et de messagerie texte. Il est tout à fait raisonnable pour une entité privée, un organisme, sans but lucratif ou peu importe, de vouloir établir une liste de contacts. Mais lorsque cela est fait à des fins politiques très claires et explicites, il faut se poser des questions au sujet de notre capacité de savoir si les personnes qui se retrouvent dans ces bases de données et qui reçoivent du contenu politique et des publicités veulent vraiment en recevoir, si l'information est fiable ou non et si les citoyens voudraient que leurs données soient retirées. Il n'y a aucun moyen réel pour les citoyens de s'approprier leurs données.

● (1220)

Le président: Merci, madame Fortier.

C'est maintenant au tour de M. Kent.

L'hon. Peter Kent: Merci, monsieur le président.

Lorsque nous parlons d'interventions étrangères et d'ingérence étrangère potentielle pendant la campagne électorale canadienne de 2019, nous avons tendance à penser à la Russie dans nos discussions. J'aimerais toutefois vous poser quelques questions sur l'histoire du Citizen Engagement Laboratory aux États-Unis qui, en 2015, en partenariat avec la fondation Tides, également établie aux États-Unis, a transféré plusieurs millions de dollars au Canada à Leadnow ou par l'entremise de sa filiale canadienne, la filiale Tides, la Sisu Institute Society en Colombie-Britannique.

Vous avez dit que 500 $ permettent d'acheter beaucoup de temps sur Facebook, alors que dire de 1,7 ou 2 millions de dollars? Je m'interroge au sujet de la réglementation. Nous revenons à l'intervention d'un tiers à propos de laquelle la chercheuse Vivian Krause, de la Colombie-Britannique, a fait remarquer qu'il est facile pour un chef politique de prendre les devants dans la campagne quand un tiers est bien financé et fait le sale boulot sur les médias sociaux.

Je me demande si vous pourriez tous les trois répondre à cette question.

Mme Elizabeth Dubois: Je ne connais pas les détails de l'affaire Leadnow. Je ne sais que ce qui a fait les manchettes. Je pense toutefois que c'est un point très important lorsque nous discutons de l'utilisation des données personnelles. Dans le cas du projet de loi C-76 qui exige une déclaration sur la protection de la vie privée, qui n'est pas très exécutoire dans le contexte de ce projet de loi et qui, à mon avis, doit être modifiée, nous ne savons pas très bien en quoi cette situation influence les relations entre ces partis et les tiers que vous avez mentionnés.

Je pense que nous devons être plus clairs à ce sujet. Je n'ai pas de recommandation précise sur la façon de résoudre ce problème, mais je pense qu'il est crucial d'intervenir.

L'hon. Peter Kent: Cela nous ramène à la question de l'ingérence étrangère.

M. Michael Pal: Je n'ai pas d'information à ce sujet. Je crois que le projet de loi C-76 exige que les tierces parties aient leurs propres comptes bancaires distincts. C'est donc une façon technique de traiter les transferts de fonds.

Sur le plan constitutionnel, vous êtes sur un terrain très solide pour limiter les dépenses. La Cour suprême en a parlé. Quant aux règles d'enregistrement et de transparence, la Cour suprême en a parlé également. Il y a aussi la question des limites des contributions, en ce qui a trait aux dons pour les partis politiques et les candidats. Ce qui est plus controversé, c'est la question de savoir s'il faut établir des limites de contribution pour les tiers.

Il est certain que la Colombie-Britannique, dans sa campagne référendaire sur la réforme électorale, a des limites quant au montant que vous pouvez verser à un commanditaire de publicité et je crois que cela s'applique également aux élections provinciales. Cela a une incidence sur l'expression politique si vous limitez le montant d'argent... Si un syndicat ou une société veut dépenser son propre argent en tant que tierce partie, comment réglementez-vous cette contribution? Il y a là des questions constitutionnelles, mais c'est une façon de régler le problème de la circulation de l'argent entre différentes entités, en le traitant comme une contribution.

L'hon. Peter Kent: Comme nous l'avons vu lors de la campagne sur le Brexit, de la campagne en faveur du Brexit, il est possible de créer des sous-groupes du tiers parti pour contourner ces limites de dépenses.

M. Michael Pal: Si vous recevez des contributions substantielles et que les limites de dépenses préétablies sont bien appliquées, alors il y a une limite quant au montant qui peut être utilisé dans cette campagne. Il y a une interaction entre les limites de contribution et les limites de dépenses.

Mme Samantha Bradshaw: Je ne suis pas une experte en ce qui a trait aux aspects juridiques entourant ce que vous pourriez faire pour empêcher les acteurs étrangers de faire des contributions à des tiers ou autres. Ce que je sais et ce que j'ai vu dans bon nombre des recherches que nous avons faites sur l'influence étrangère dans d'autres pays, c'est qu'ils ont tendance à travailler avec beaucoup de mouvements nationalistes qui sont déjà en place.

Aux États-Unis, par exemple, il a toujours été difficile de différencier la rhétorique d'un influenceur russe de celle des membres des organisations de droite. Une grande partie de ces éléments vont de pair et ils travaillent ensemble pour créer une sorte de rhétorique commune. Je pense toutefois qu'il y a des choses que nous pourrions faire pour réglementer ce problème. M. Pal a soulevé de bons points. Je ne pense pas que cela va disparaître complètement, mais il s'agit d'augmenter les coûts pour ces acteurs étrangers et d'autres influenceurs. De cette façon, il est un peu plus difficile pour eux de commencer à influencer les électeurs.

Je pense que la transparence quant à la provenance des fonds, à la proportion des fonds dépensés et à l'usage qui en est fait contribuerait à créer un peu plus de responsabilisation dans le système politique.

● (1225)

Le président: Merci.

La parole est maintenant à Mme Vandenbeld, pour cinq minutes.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci à vous tous d'être ici. Votre témoignage est extrêmement éclairant.

J'aimerais prendre un peu de recul et réfléchir à ce dont nous parlons exactement lorsque nous parlons de robots, de cyborgs et d'intelligence artificielle. Je pense que nous avons tous une petite idée de ce que nous voulons dire, mais pourrions-nous examiner des exemples précis?

Par exemple, madame Bradshaw, vous avez dit avoir interviewé des développeurs de robots. Qu'est-ce que cela signifie: mettre au point un robot? En quoi cela consiste-t-il? Vous avez dit qu'il y aurait des principes, comme la viralité ou la pertinence et que vous pourriez mettre des principes qui soutiennent la démocratie dans un robot quand vous le développez. Pouvez-vous nous expliquer ce que cela signifie exactement?

Mme Samantha Bradshaw: Oui. Lorsque je parlais des principes qui sous-tendent les algorithmes, je parlais davantage des algorithmes des médias sociaux et de la façon dont ils adaptent le contenu ou le livrent aux utilisateurs. Ils offrent du contenu selon la viralité. Si les éléments obtiennent beaucoup de clics, cela suscite donc l'intérêt d'un grand nombre de personnes et, par conséquent, pourrait provoquer une tendance. C'est un peu ce dont je parlais.

Au lieu des principes entourant la viralité, nous voulons peut-être des principes sur l'information factuelle provenant des médias professionnels plutôt que des sources qui produisent constamment des nouvelles trompeuses ou bidon. Les médias professionnels devraient peut-être avoir — le mot technique ne me vient pas à l'esprit en ce moment —, mais ils devraient en faire une priorité dans les algorithmes. C'est à cela que je faisais allusion lorsque je parlais de concevoir des algorithmes pour la démocratie. Cela change ce genre de principes.

En ce qui concerne les développeurs de robots... Ce n'était pas mon projet de recherche de base, mais je peux vous recommander un des chercheurs qui a fait beaucoup plus d'entrevues que moi à ce sujet. Il s'appelle Sam Woolley. Il a constaté que les développeurs de robots sont semblables aux autres développeurs de technologies dans leur approche. Ils créent un logiciel conçu pour imiter le comportement humain, capable d'amplifier une nouvelle. Il pourrait également converser avec les utilisateurs en ligne.

Les robots sont capables de plusieurs interactions différentes. Cela dépend vraiment des objectifs du concepteur. Les développeurs ont peut-être des idéaux ou des principes qu'ils intègrent aux robots. Beaucoup d'entre eux considèrent que ces robots sont efficaces pour la démocratie parce qu'ils contribuent à amplifier un message qui pourrait ne pas être entendu ou qui pourrait suivre une tendance sans l'aide du robot.

Mme Anita Vandenbeld: Mme Dubois aimerait intervenir.

Mme Elizabeth Dubois: Les robots politiques sont des comptes automatisés, que l'on trouve parfois sur les médias sociaux, parfois sur Instagram, parfois sur Twitter, parfois dans des applications de messagerie instantanée. Il y a toutes sortes d'endroits où les robots politiques interagissent.

Il y a d'autres types de robots qui utilisent les données numériques pour faire des choses comme s'assurer que Wikipédia est à jour. Il y a différents types de robots, mais quand je parle de robots politiques, je parle de ceux qui interagissent avec les humains. Ils imitent les humains d'une certaine façon. Les gens qui créent ces robots ont peut-être beaucoup de compétences techniques. Il peut s'agir d'informaticiens et de développeurs. Il pourrait aussi s'agir de gens qui utilisent des outils qui ont été mis au point par un autre développeur pour créer rapidement des robots. Il n'est pas nécessaire d'avoir beaucoup de compétences techniques pour mettre un robot en marche.

Il faut aussi se rappeler qu'il y a des entreprises entières — en fait, une industrie — qui reposent sur l'idée de l'optimisation de moteurs de recherche qui utilisent certaines de ces techniques et qui pourraient utiliser un réseau de robots qu'elles ont créé. Par exemple, il pourrait y avoir toute une série de robots qu'elles créent sur Twitter pour que tous interagissent entre eux afin d'amplifier un message. Il y aurait peut-être une organisation derrière la mise au point de ces robots et vous pourriez en faire profiter, comme mon collègue l'a expliqué, la personne même qui a rédigé le code à l'origine.

● (1230)

Mme Anita Vandenbeld: Madame Dubois, vous avez notamment parlé des gens qui manipulent les algorithmes. Je pense que vous avez même parlé de casser un algorithme. Qu'est-ce que cela signifie?

Mme Elizabeth Dubois: Manipuler un algorithme serait... L'exemple typique est l'optimisation des moteurs de recherche. Disons qu'un événement se déroule à Ottawa. Nous voulons que le mot-clic de cet événement se propage à Ottawa afin que quiconque se trouve dans la région d'Ottawa puisse voir le mot-clic sur sa petite barre de tendance de Twitter. L'idée pourrait être de créer tout un tas de robots qui partagent du contenu en utilisant ce mot-clic pour augmenter artificiellement son importance sur Twitter, de sorte que l'algorithme de tendance de Twitter l'oblige à le mettre à l'avant-plan pour que les gens le voient. Ce serait une forme de manipulation de l'algorithme.

Casser l'algorithme, ce serait le manipuler jusqu'à ce que l'entreprise qui a créé l'algorithme au départ soit obligée de le remanier totalement parce qu'il ne fait plus ce qu'il est censé faire.

Le président: Merci.

Madame Vandenbeld, votre temps est écoulé.

Nous allons avoir une autre série de questions après celle-ci, mais la dernière intervention de la présente série de trois minutes revient à M. Angus.

M. Charlie Angus: Merci.

Ce qui a déclenché toute cette enquête, c'est l'énorme atteinte à la confidentialité de Facebook qui a mené à Cambridge Analytica et la possibilité que cette information ait nui au vote sur le Brexit. Il y a eu une autre atteinte à la sécurité de 50 millions d'utilisateurs sur Facebook. Nous n'en avons aucune idée. On nous dit de ne pas nous inquiéter. D'après ce qu'ils peuvent voir, tout va bien.

Dès que j'ai entendu cela, je me suis dit: « Super, Dieu merci, nous avons Facebook sur le dossier. Il n'y a pas lieu de s'inquiéter. »

Lorsque nous avons reçu les représentants de Facebook ici, nous avons posé des questions sur les meurtres en masse qui ont eu lieu au Myanmar. Ce n'est pas la responsabilité de Facebook qu'il y ait eu des meurtres de masse, mais Facebook a été accusé à maintes reprises de ne pas réagir à l'utilisation abusive de sa plateforme. Les représentants ont répondu quelque chose comme: « Nous le reconnaissons, nous ne sommes pas parfaits. » Nous parlons du pouvoir d'une plateforme de se livrer à des tueries.

Nous parlons de beaucoup d'ajustements à un système qui semble soudainement plus puissant, plus englobant que le droit interne, que tout ce que nous avons connu dans le passé, et cela semble dépasser de nombreuses compétences avec très peu de respect. Croyez-vous que des plateformes comme Facebook, comme Google, doivent être réglementées, ou pouvons-nous leur faire confiance pour réagir lorsqu'il y a suffisamment d'indignation? Faut-il prendre des mesures antitrust pour les casser, puisque Facebook contrôle maintenant Instagram, WhatsApp et de nombreuses autres plateformes? C'est la même chose avec Google.

Que pensez-vous de la possibilité de demander des comptes à ces entreprises? Est-ce de l'autoréglementation? Est-ce de l'antitrust? Est-ce une forme de réglementation nationale ou internationale? La question est posée.

Mme Samantha Bradshaw: Je vais intervenir en premier. Pour moi, c'est un peu de tout. Nous avons certainement besoin d'une réglementation. Si la dernière année nous a appris quelque chose, c'est que nous devons intervenir, et le gouvernement a un rôle vraiment important à jouer dans la réglementation de ces plateformes.

Je pense que l'autoréglementation du secteur privé est également une question importante à régler. Pour ce qui est de votre exemple concernant le Myanmar et la façon dont Facebook a causé beaucoup de fausses nouvelles et de désinformation qui ont mené à la violence et à la mort, je pense que c'est un problème réel et grave. Comme vous l'avez dit, nous avons des entreprises qui exercent leurs activités à l'échelle mondiale, mais elles n'ont pas de personnel dans chaque pays qui s'occupe de la modération du contenu pour régler beaucoup de problèmes très locaux.

Avoir un modérateur de contenu en Californie qui ne connaît rien de l'histoire et de la culture du Myanmar ou du Sri Lanka, ou de beaucoup d'autres pays où il y a des tensions ethniques et qui prend des décisions sur le contenu, c'est vraiment un gros problème. Pourtant, Facebook a du personnel publicitaire dans beaucoup de ces pays. Alors, je pense que le fait d'intensifier la modération du contenu et de la rendre plus mondiale et inclusive est une bonne mesure d'autoréglementation du secteur privé que les gouvernements pourraient aussi mettre en vigueur sur les plateformes.

● (1235)

Mme Elizabeth Dubois: Je pense que l'autoréglementation est absolument insuffisante. Ce que Facebook, en particulier, a fait en réaction aux pressions qu'on exerce actuellement sur cette entreprise est bon. Nous devons continuer de voir ces choses.

M. Pal a donné l'exemple de la création volontaire d'un dépôt de certaines publicités électorales. Oui, c'est très bien, et je suis heureuse que cela se produise, mais comme M. Pal l'a aussi mentionné, ces entreprises pourraient nous enlever cela et nous n'aurions absolument aucun recours. Élections Canada serait alors vulnérable parce qu'il déciderait de se fier à quelque chose qui n'est pas prévu par la loi. Si ce dépôt est supprimé pendant une élection, notre démocratie et notre système démocratique courent un risque énorme.

Il faut aussi se rappeler que ce sont de grandes entreprises internationales. Elles n'auront pas à l'esprit les particularités de la population canadienne lorsqu'elles concevront leur autoréglementation. Pour ce qui est de la population canadienne, nous avons de grandes régions du Nord du Canada qui comptent beaucoup sur Facebook comme principale source d'information politique. Si Facebook n'est pas en mesure de prêter attention aux nuances des populations autochtones du Canada et à la façon dont elles échangent de l'information, alors ces personnes risquent d'être mal desservies d'une façon qui va à l'encontre de notre démocratie et qui risque de les marginaliser vraiment.

Pourquoi nous attendrions-nous à ce que les dirigeants de Facebook qui prennent des décisions sur la façon dont Facebook sera déployé partout dans le monde comprennent le contexte canadien dans ces domaines particuliers? Il serait déraisonnable, à mon avis, de leur demander de s'en occuper. En fait, il faut que ce soit le gouvernement canadien qui défende les citoyens canadiens.

Le président: Nous arrivons à la fin de notre première série de questions.

Je vais poser une question aux témoins, si vous me le permettez.

Par le passé, nous avons parlé des comptes anonymes sur Facebook et des plateformes qui... Ils se cachent dans l'ombre. Ce sont des robots ou de vraies personnes qui se cachent dans l'ombre. Devrait-il même être possible de se cacher dans l'ombre et de ne pas être une entité publique? Il me semble que ce serait un choix évident. Un algorithme ne pourrait pas se faire passer pour quelqu'un qui n'est pas là, s'il n'y était pas. Il faudrait qu'il s'agisse d'une vraie personne qui s'occupe de ce dossier ou de ce programme en particulier, etc., qui l'utilise vraiment. Pensez-vous que c'est possible ou est-ce quelque chose à envisager? Qu'en pensez-vous?

Mme Elizabeth Dubois: L'un des principaux problèmes de ce que nous pourrions appeler une telle « couche d'établissement de l'identité », c'est ce qui devient la vérification de la véritable identité de la personne. Airbnb vous demande de prendre une photo de votre passeport ou de votre permis de conduire. Je ne suis pas très à l'aise avec le fait qu'Airbnb ait une copie de mon passeport lorsque j'ai ouvert une session sur Facebook et que j'ai ensuite eu accès à 50 millions de comptes d'utilisateur. Il y a des conséquences importantes qui pourraient vraiment poser problème sur le plan de la protection de la vie privée et de la sécurité des données personnelles.

On se demande également si l'anonymat réglerait certains de ces problèmes. Nathan — j'oublie son nom de famille — est au MIT, où il a rédigé une étude très intéressante sur le rôle de l'anonymat et sur la question de savoir si cela aide dans les cas de discours haineux et de désinformation. En fait, l'élimination de l'anonymat ne résoudrait pratiquement rien de ces problèmes. Cette solution pourrait donc poser problème.

Le président: Mme Bradshaw a quelque chose à ajouter.

Mme Samantha Bradshaw: Je suis d'accord. Je pense qu'il y a un risque réel à retirer l'anonymat de ces plateformes. Il ne faut pas oublier qu'il s'agit de plateformes mondiales. Protéger l'identité des personnes dans les pays où la liberté d'expression est moindre et où la protection contre les violations des droits de la personne est moindre... Les gens comptent sur l'anonymat de ces plateformes pour communiquer, délibérer et organiser des manifestations.

Je pourrais faire le lien avec les petits comptes vérifiés de Twitter. Si, par exemple, les comptes étaient vérifiés comme étant ceux d'une personne réelle, cela pourrait rendre les faux comptes encore plus puissants, parce qu'ils ont maintenant passé ce filtre et que les gens auront tendance à faire davantage confiance à ces sources. Ils pourraient en fait être plus efficaces pour répandre la désinformation.

● (1240)

Le président: C'est intéressant.

Monsieur Pal.

M. Michael Pal: Je pense que la proposition selon laquelle l'anonymat peut être important pour faciliter l'expression politique est un très bon point. Je pense que cela s'applique aussi au Canada, dans certaines circonstances. Je dirais que si vous dépensez de l'argent pour quelque chose qui compte comme de la publicité électorale en vertu de la définition de la Loi électorale, il devrait y avoir une certaine vérification de la source, c'est-à-dire qu'il s'agit d'une personne réelle et d'un acteur national. C'est différent si vous voulez simplement vous exprimer politiquement sur Twitter et critiquer un politicien. Il est utile de permettre l'anonymat.

C'est là que je tracerais la ligne. Cela peut être difficile à appliquer. Si vous dépensez de l'argent pour de la publicité, le public devrait avoir le droit de savoir.

Le président: Merci.

Pour la prochaine série de questions, j'ai M. Baylis pour sept minutes.

Allez-y, monsieur Baylis.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Je vais reprendre exactement là où vous avez terminé, monsieur Pal. J'aimerais que vous répondiez tous les trois à cette question. Je vais commencer par essayer de faire ce que vous avez dit, madame Dubois, c'est-à-dire définir une publicité politique.

Je vois les choses de deux façons. Si je suis resté chez moi, que j'ai écrit un article et que je l'ai publié sur Facebook ou Twitter ou ailleurs, et que les gens commencent à le partager, que j'aie 100 amis ou 10 000 amis, je l'ai simplement publié. Si je prends le même article et que je paie 10 $ pour le faire afficher quelque part, je fais valoir que ce n'est plus un avis personnel, mais une annonce. J'aimerais savoir s'il s'agit d'une première ligne de délimitation que nous pourrions faire pour dire: « Il s'agit d'une publicité. Ce n'est pas une publicité. »

Monsieur Pal, vous pourriez peut-être commencer.

M. Michael Pal: Il y a une définition de la publicité dans la Loi électorale, c'est-à-dire message favorisant ou contrecarrant un parti ou un candidat, directement ou indirectement, ou une prise de position sur une question à laquelle ils sont associés. Nous pouvons travailler à partir de là.

M. Frank Baylis: Mais le fait d'être payé ou non...

M. Michael Pal: Certains systèmes, un système fédéral, ont un montant d'argent, alors le projet de loi C-76 va éliminer ce montant pour la publicité des entités étrangères, mais il serait toujours là pour les entités nationales. La Colombie-Britannique n'avait pas de montant d'argent et la Cour suprême du Canada a récemment été saisie d'une affaire pour essayer d'interpréter ce que cela signifie si vous achetez des crayons à dessiner et que votre enfant place une pancarte politique dans la fenêtre. Par conséquent, je pense qu'il est utile d'avoir une sorte de seuil monétaire. Cela pourrait mettre fin à l'application excessive de petites publicités politiques.

Mme Elizabeth Dubois: Je pense que la distinction entre le contenu payant et le contenu non payé est utile. Je pense qu'il faut aussi se rappeler que le contenu est important pour décider si c'est politique ou non. C'est la diffusion du contenu qui en fait de la publicité. Vous pourriez payer un artiste pour créer un message de campagne politique que vous laissez dans votre maison. C'est payé et c'est politique, mais ce n'est pas diffusé. La distinction est importante parce que les choses qui aident à diffuser du contenu qui n'a pas été payé, je pense, pourraient encore raisonnablement être considérées comme de la publicité.

Imaginez que quelqu'un écrit un message sur Twitter, qu'il ne paie pas lui-même pour le faire promouvoir, mais que quelqu'un d'autre décide de le faire...

M. Frank Baylis: J'aimerais y revenir, mais commençons par eux.

La première chose, c'est que j'écris un billet et je le mets là. Je n'ai pas fait de publicité si je n'ai pas payé.

Mme Elizabeth Dubois: C'est exact.

M. Frank Baylis: Je vais revenir sur ce deuxième point.

Madame Bradshaw.

Mme Samantha Bradshaw: Je n'ajouterai pas grand-chose à la conversation, sauf que je pense que la distinction entre quelque chose qui est payant et quelque chose que je publie naturellement est une bonne façon de définir une publicité.

M. Frank Baylis: D'accord, alors revenons à la deuxième étape. Tout d'abord, nous disons qu'il y a un seuil monétaire. Ce seuil devrait peut-être être abaissé parce que son impact pourrait être plus élevé. Nous disons: « C'est une publicité payée. Ce n'est pas une publicité payée. » Tout à coup, quelqu'un arrive avec un robot et dit que cet homme a écrit un excellent article dans sa maison, qu'il l'a transmis à 10 amis et que nous voulons diffuser ce message. Donc, le robot se met au travail ou je commence à payer. Ensuite, j'ai converti cela en publicité à mon stade, ou même si je disais tout simplement à un robot de faire une recherche sur Internet, de trouver ce bon message et de le diffuser, cela signifie que cela passe d'une publicité non payée, quand je l'affiche, à une publicité informatisée.

Est-ce que c'est aussi à ce point-là qu'on pourrait dire qu'il s'agit maintenant d'une publicité payante?

● (1245)

Mme Elizabeth Dubois: M. Pal aurait une meilleure idée de ce qui se passerait en vertu de la loi actuelle. Je pense que ce devrait être le cas, la mise en garde étant que ce ne serait pas la personne qui a créé le contenu au départ qui devrait être tenue responsable, mais plutôt la personne qui a payé pour que ces robots soient dirigés vers ce contenu.

M. Frank Baylis: Vous parlez de la personne qui a converti quelque chose en publicité.

Mme Elizabeth Dubois: Oui.

M. Frank Baylis: Très bien.

Monsieur Pal.

M. Michael Pal: Élections Canada a une note d'interprétation sur la publicité politique en ligne. On dit que pour être compté comme de la publicité électorale, l'article doit avoir un coût de placement. La question juridique est de savoir s'il y a eu de l'argent et une transmission, mais il faut aussi qu'il y ait un coût de placement, qui est différent, disons, à la télévision ou à la radio. Je suppose que la question est de savoir si cela compte comme un coût de placement ou non.

Nous voulons être prudents et ne pas restreindre la capacité d'échanger des renseignements de façon naturelle.

M. Frank Baylis: Nous ne le partageons pas de façon naturelle. Ce que nous disons, c'est qu'il est passé de quelque chose de naturel à quelque chose de professionnalisé. Dès qu'un robot intervient ou qu'une autre personne paie, nous passons d'un processus purement interne à un processus professionnalisé. Dans ce cas, vous dites qu'il y a un coût de placement.

Disons que j'ai conçu une application et que je l'ai mise sur le marché et qu'elle faisait ce qu'elle voulait sans moi. Est-ce que cela serait couvert par ce coût de placement, ou est-ce qu'on devrait adapter la loi?

M. Michael Pal: J'aimerais en savoir davantage sur les faits, mais je ne le crois pas. Le régime des coûts de placement ne fonctionne pas parfaitement lorsqu'il est question d'augmenter le nombre de messages et de les communiquer au moyen de robots ou de cyborgs.

M. Frank Baylis: C'est ce que j'appelle communiquer à l'aide d'un processus professionnalisé, par opposition à un processus naturel. Oublions que Facebook existe et disons, par exemple, que je parle à mon ami. Il dit que c'est une excellente idée, Frank, et il parle à ses amis. Il n'y a rien d'illégal là-dedans.

Disons que nous avons défini ce qui est une publicité et ce qui n'en est pas. Vous avez tous parlé de plusieurs éléments du contrôle d'une publicité. Je n'ai pas beaucoup de temps, et je suis d'accord avec le dépôt public. Quelqu'un est-il en désaccord avec cela? Parfait.

Je suis d'accord pour qu'on indique qui est l'agent officiel et qui a payé. Je suis d'accord avec l'idée que les tarifs publicitaires devraient être les mêmes que ceux que nous avons actuellement, afin qu'ils ne puissent pas par inadvertance promouvoir un point de vue.

Vous avez soulevé un point sur lequel je ne suis pas d'accord, c'est-à-dire la transparence quant aux raisons pour lesquelles l'électeur a été ciblé. Disons que je reviens aux feuilletons. Les feuilletons sont apparus dans les années 1930. Les gens avaient des radios, et les annonceurs se demandaient qui ils allaient cibler. Ils voulaient cibler les femmes, parce que les femmes allaient rester à la maison. Ils ont écrit le contenu pour les femmes et ils l'ont diffusé quand ils savaient que les femmes étaient seules à la maison. Ils leur vendaient de tout, surtout des choses dont elles avaient besoin à la maison.

Je ne vois pas de problème à ce que quelqu'un me cible comme tel. J'aimerais savoir ce que vous en pensez, en commençant par vous.

M. Michael Pal: La question de politique publique, c'est que les électeurs pourraient se sentir profondément offensés par les termes de recherche précis utilisés pour les cibler. Cela s'explique en partie par le fait que ces personnes ne savent pas nécessairement quelles sont les données que possèdent les entités qui les ciblent par leur publicité.

Comme utilisateur de Facebook, il est très difficile de savoir quelle information Facebook a à votre sujet. Il se trouve que si vous vous connectiez à Facebook en utilisant l'authentification à deux facteurs, Facebook l'utilisait et donnait des renseignements supplémentaires aux annonceurs. C'est ce que nous avons appris lors de la récente intrusion touchant au moins 50 millions de personnes. Cela revient à l'idée que vous devriez avoir le plus d'information possible sur la façon dont vous êtes maintenant inclus dans le processus politique, d'autant plus qu'il y a un intérêt public à ce que la publicité politique fonctionne selon des modalités qui, nous en convenons, sont légitimes dans un système démocratique.

Si vous vendez des chaussures, les termes de recherche utilisés ne me dérangent pas autant. Si vous ciblez des gens parce que vous pensez qu'ils sont racistes ou que vous pouvez peut-être les encourager à être plus racistes, vous ne pouvez pas le faire sur une publicité à l'émission *Hockey Night in Canada* parce que vous allez être mis à contribution, n'est-ce pas? Tout le monde la voit.

Cependant, si l'information est microciblée sur une personne, il n'y a pas cet élément public, alors il nous incombe de donner plus d'information à la personne, de lui permettre de faire cette évaluation.

Le président: Notre temps est écoulé. Je suis désolé, mais c'est vraiment serré pour les sept dernières minutes. Je dois passer à quelqu'un d'autre.

Monsieur Kent, vous avez sept minutes.

L'hon. Peter Kent: Merci beaucoup, monsieur le président.

J'ai été impressionné par le fait que vous avez tous dit aujourd'hui, de différentes façons, que nous devrions être prudents au sujet de la surréglementation en ce qui concerne le monde numérique, les médias sociaux et les données personnelles accumulées dans le processus électoral. Je me demande dans quelle mesure les électeurs devraient être informés de ce que les partis politiques ont sur eux ou de ce que les partis politiques considèrent comme leur tendance lorsqu'ils votent.

Après tout, le porte-à-porte, le contact en personne, est encore là aujourd'hui. Autrefois, c'était aussi le téléphone, mais en l'absence de lignes terrestres, cette méthode a disparu, comme le dronte de Maurice. Quand on fait du porte-à-porte dans une circonscription ou une autre, on découvre qui est porté à voter pour le parti pendant la période électorale ou pendant toute la session parlementaire.

Le jour de l'élection, nous voulons que les gens aillent voter, alors notre encouragement, notre message, d'une façon ou d'une autre, s'adresse à ceux que nous savons susceptibles d'appuyer l'un ou l'autre de nos partis. Ce n'est pas que nous décourageons les autres qui, à la porte, nous ont dit qu'ils ne votent pas pour nous, mais pour le parti X ou le parti Y. C'est simplement que nous allons là où se trouvent les votes. Nous ne gaspillons pas notre énergie à essayer d'encourager les gens à aller voter pour nous.

Encore une fois, pour en venir au concept épineux de l'identité dans le monde numérique ou dans le monde des données accumulées, serait-il nécessaire de dire à un électeur que nous le considérerions comme étant tiède de m'appuyer comme candidat ou peut-être même hostile et très peu susceptible de voter pour moi ou pour mon parti? Comment peut-on divulguer cette information? De plus, n'y aurait-il pas beaucoup de travail à faire si les gens exigent de savoir ce que le parti pense d'eux ou comment il les considère?

● (1250)

Mme Elizabeth Dubois: Oui, je pense que c'est une question importante. Pour ce qui est de la comparaison avec la collecte de données actuelle par rapport à ce qui se faisait lorsque le porte-à-porte et le téléphone étaient vraiment la seule option, alors les gens savaient à un certain niveau quelles données étaient recueillies sur eux parce qu'on leur posait la question. Ils ont dû les donner à quelqu'un qui les écrivait sur sa planchette à pince.

L'hon. Peter Kent: Oui.

Mme Elizabeth Dubois: C'est une distinction importante. Il faut se demander si cela va créer beaucoup de travail, qui constituera un fardeau injuste pour les partis. À tout le moins, ce que j'ai suggéré comme nécessaire serait le niveau supérieur... Cela reviendrait à dire que comme parti, voici les données que nous recueillons et voici les sources. Nous recueillons donc des renseignements sur les personnes pour lesquelles vous dites que vous allez voter si vous le mentionnez, et nous recueillons de l'information sur votre numéro de téléphone. Voilà comment nous allons les obtenir. Vous dites cela.

Ensuite, pour ce qui est d'avoir un mécanisme permettant aux gens de vérifier ce qu'il en est et de corriger l'information erronée, je pense que cela devient une question plus vaste, où nous commençons à nous demander si nous voulons adopter l'approche du RGPD. Est-ce ce vers quoi le Canada devrait tendre? Je ne suis pas une experte du RGPD, alors je ne peux pas vraiment parler de la mise en oeuvre précise de ce mécanisme, mais du point de vue d'un parti politique, il est important d'avoir une déclaration minimale qui indique « voici les données que nous essayons de recueillir à votre sujet et voici comment nous allons les obtenir ».

M. Michael Pal: Je pense que les mécanismes de protection des renseignements personnels des électeurs sont importants. Il est toutefois juste pour les partis politiques de dire qu'ils ont besoin d'un mécanisme pour éliminer les demandes frivoles ou vexatoires qui sont là simplement pour accaparer toutes les ressources des partis politiques. Vous pouvez imaginer un autre parti politique envoyer un tas de gens demander leurs renseignements personnels tous les jours, n'est-ce pas? Ce n'est pas un scénario trop fantaisiste.

La plupart des autres entités de la société canadienne qui ont des quantités importantes de données respectent les règles sur la protection des renseignements personnels. C'est une bonne question quant à la façon exacte de les concevoir. Je pense qu'il est juste d'éliminer les plaintes frivoles, mais je pense que cela peut encore se faire pour les partis politiques.

L'hon. Peter Kent: Madame Bradshaw?

Oh, nous avons perdu votre audio.

Mme Samantha Bradshaw: J'ai manqué la majeure partie de la question à cause de l'interruption. Pourriez-vous résumer rapidement?

L'hon. Peter Kent: Combien de renseignements les partis politiques, les campagnes politiques individuelles, devraient-ils divulguer au sujet de ce qu'ils savent sur un électeur qui appuie un parti ou un candidat ou qui s'y oppose?

Mme Samantha Bradshaw: Quels que soient les renseignements que les partis politiques recueillent sur des électeurs potentiels, ils devraient être divulgués. Comme d'autres témoins l'ont dit, d'autres entités déclarent déjà cette information en vertu de la loi, et les partis politiques ne devraient pas faire exception. Il est vraiment important que les utilisateurs comprennent aussi que ce sont les données que ces entités ont à leur sujet.

● (1255)

L'hon. Peter Kent: Le problème, c'est que lorsqu'on frappe à une porte, on obtient parfois une réponse enthousiaste favorable ou parfois très négative, mais je dirais que dans de nombreuses élections, on obtient les indécis, et il y a des nuances dans les indécis: « Eh bien, cela m'intéresse » ou « Je penche... », etc. Cela se résume à la façon dont les partis seraient tenus de consigner le contact en personne qu'ils obtiennent et de l'exprimer aux gens sans être offensants ou, comme M. Pal l'a laissé entendre, de les soumettre à des demandes de renseignements vexatoires pendant des jours et des jours, simplement comme un exercice qui demande beaucoup de temps et de ressources.

Mme Samantha Bradshaw: Là où j'aimerais voir des améliorations, c'est au niveau des rapports sur les raisons pour lesquelles je serais ciblée en premier lieu, parce que comparativement au fait de frapper aux portes, ou même d'utiliser d'autres technologies comme la télévision ou la radio, ce genre d'interaction ne fournit pas la même richesse d'information que les médias sociaux recueillent sur les gens. Pour situer cela dans votre contexte monétaire, Google vient de payer 9 milliards de dollars pour que Google Search soit la valeur par défaut des appareils Apple. Voilà à quel point les données recueillies à notre sujet sur ces plateformes sont précieuses. Cela peut en dire beaucoup, et c'est pourquoi je pense qu'il est vraiment important d'avoir plus de transparence quant aux raisons pour lesquelles nous sommes ciblés, pour quelles raisons. Cela change les décisions des gens.

Le président: Merci, monsieur Kent.

Le dernier intervenant est M. Angus.

M. Charlie Angus: Merci.

C'est fascinant. Comme vous pouvez le constater, il s'agit d'un sujet très complexe. Nous voulons en faire un rapport que nous pourrons présenter au Parlement avec des suggestions opportunes qui ne portent pas atteinte au droit des gens de se chicaner sur Facebook ou de troller des politiciens qu'ils n'aiment pas. C'est un droit démocratique. Nous voulons également nous assurer que les droits des gens ne sont pas injustement brimés par la manipulation des données.

Vous avez tous formulé de très bonnes recommandations générales, mais y a-t-il des recommandations précises que nous devrions prendre en considération dans notre rapport? Si vous pouviez mettre cela par écrit et nous le faire parvenir, ce serait très utile, parce que je pense que nous nous dirigeons vers quelque chose que nous voulons présenter au Parlement. Vos recommandations sont excellentes, mais s'il y a des détails, veuillez nous les faire parvenir.

Merci.

Le président: J'abonde dans le même sens que M. Angus. Veuillez nous faire part de vos idées et suggestions et nous essaierons de les inclure dans le rapport pour ce que nous considérons comme l'avenir de notre démocratie.

En ma qualité de président, je tiens à vous remercier tous d'être venus aujourd'hui.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur.* Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur.*

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes
à l'adresse suivante : http://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act.* Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act.*

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the
following address: http://www.ourcommons.ca